POLICY STATEMENT
Commonwealth of Pennsylvania • Department of Corrections

Policy Subject:		Policy Number:
Information Technology		**2.3.1**
Date of Issue:	**Authority:**	**Effective Date:**
October 28, 2010	**Signature on File** **Shirley Moore Smeal**	**November 5, 2010**

I. AUTHORITY

A. The Authority of the Secretary of Corrections to direct the operation of the Department of Corrections is established by Sections 201, 206, 506, and 901-B of the Administrative Code of 1929, 71 P.S. §§61, 66, 186, and 310-1, Act of April 9, 1929, P.L. 177, No. 175, as amended.

B. By way of a Memorandum of Understanding (MOU) between the Department, PA Board of Probation and Parole (PBPP), the Office of the Victim Advocate (OVA), the Sex Offender Assessment Board (SOAB) and the Firearms Education and Training Commission (FETC), dated September 27th, 2007, the parties agreed that in the interest of achieving operational efficiencies, the Department provides information technology services and functions to the PBPP, OVA, SOAB and the FETC.

C. Section 2.2.1 of the MOU states that the parties involved will "develop and implement information technology policy, procedures and business processes that reflect the current organizational needs and requirements of the PBPP and the Agencies." Therefore, this policy and procedure will be subject to review and comment from the applicable Agency Heads prior to being signed by the Secretary of Corrections.

II. APPLICABILITY

This policy is applicable to all facilities operated under the jurisdiction of, or conducting business with the Department, PBPP, OVA, SOAB and the FETC. The use of the word "Agency" or "Agencies" throughout this policy refers collectively to the aforementioned entities.

III. POLICY

It is the policy of the Agencies to:

A. provide appropriate individuals access to IT equipment, software and systems for the conduct of Commonwealth business and Agency sanctioned education, training, or other approved purposes;

B. ensure the integrity and security of information and equipment, software and systems; and

C. ensure that all persons using Commonwealth owned or leased equipment, software, and systems comply with all applicable copyright laws and Commonwealth/Agency policy and procedures relating to information technology.

IV. PROCEDURES

All applicable procedures are contained in the procedures manual that accompanies this policy document.

V. SUSPENSION DURING AN EMERGENCY

In an emergency or extended disruption of normal facility operation, the Secretary/designee may suspend any provision or section of this policy for a specific period.

VI. RIGHTS UNDER THIS POLICY

This policy does not create rights in any person nor should it be interpreted or applied in such a manner as to abridge the rights of any individual. This policy should be interpreted to have sufficient flexibility to be consistent with law and to permit the accomplishment of the purpose(s) of the policies of the Department of Corrections.

VII. RELEASE OF INFORMATION AND DISSEMINATION OF POLICY

A. Release of Information

1. Policy

   This policy document is public information and may be released upon request.

2. Confidential Procedures (if applicable)

   Confidential procedures for this document, if any, are <u>not public information</u> and may not be released in its entirety or in part, without the approval of the Secretary of Corrections/designee. Confidential procedures may be released to any Department of Corrections employee on an as needed basis.

B. Distribution of Policy

1. General Distribution

   The Department of Corrections' policy and procedures shall be distributed to the members of the Central Office Executive Staff, all Facility Managers, and Community Corrections Regional Directors on a routine basis. Distribution of confidential procedures to other individuals and/or agencies is subject to the approval of the Secretary of Corrections/designee.

2. Distribution to Staff

   It is the responsibility of those individuals receiving policies and procedures, as indicated in the "General Distribution" section above, to ensure that each employee expected or required to perform the necessary procedures/duties is issued a copy of the policy and procedures either in hard copy or via email, whichever is most appropriate.

VIII. SUPERSEDED POLICY AND CROSS REFERENCE

A. Superseded Policy

1. Department Policy

   2.3.1, Information Technology, issued July 1, 2009, by Secretary Jeffrey A. Beard, Ph.D.

2. Facility Policy and Procedures

   This document supersedes all facility policy and procedures on this subject.

B. Cross Reference(s)

1. Administrative Manuals

   a. DC-ADM 003, Release of Information;

   b. DC-ADM 801, Inmate Discipline;

   c. 3.1.1, Fiscal Administration;

   d. 6.3.1, Facility Security;

   e. 8.1.1, Community Corrections Centers; and

   f. PBPP Operations Manual.

2. ACA Standards

   a. Administration of Correctional Agencies: 2-CO-1F-06

   b. Adult Correctional Institutions: 4-4101

   c. Adult Community Residential Services: None

   d. Correctional Training Academies: None

3. Other

   The Management Directives and Information Technology Bulletins referenced below may be accessed through DOCNet:

   http://www.portal.state.pa.us/portal/server.pt/community/docnet/16071

   or the associated OA site noted below.

   a. Office of Administration (OA)

      http://www.portal.state.pa.us/portal/server.pt/community/management%20directives/711/management_administrative_support_%28205-260%29/208571

      (1) MD 205.34 – Commonwealth of Pennsylvania Information Technology Acceptable Use Policy;

      (2) MD 210.5 – The Commonwealth's Enterprise Records Management Program;

      (3) MD 210.15 – Instant Messaging;

      (4) MD 240.11 – Commonwealth Wireless Communication Policy; and

      (5) MD 245.18 – IT Administrator Acceptable Use, Auditing and Monitoring, Incident Notification and Response Policies and Procedures.

   b. OA/Office for Information Technology (OA/OIT)

      http://www.portal.state.pa.us/portal/server.pt/community/policies_procedures/10048

      Information Technology Bulletins (ITBs) are issued by OA/OIT as enterprise technology policies and standards for all agencies under the Governor's jurisdiction. The following policies, included, are specifically referenced:

      (1) ITB-APP011 – Application Development Languages;

      (2) ITB-APP020 – Open Source Software;

(3) ITB-INF001 – Database Management Systems;

(4) ITB-INFRM006 – Electronic Document Management Systems;

(5) ITB-INFRM007 – Management of Electronic Information Created via Multi-Functional Devices or Other Non-EDMS Desktop Scanners;

(6) ITB-NET001 – Wireless LAN Technology;

(7) ITB-SEC010 – Virtual Private Network Policy;

(8) ITB-PLT001 – Desktop and Laptop Technology Standards;

(9) ITB-SYM006 – Desktop and Server Software Patching Policy;

(10) ITB-SYM009 – Commonwealth of Pennsylvania Data Cleansing Policy;

(11) ITB-PLT010 – CoPA Policy for the Management of Networked Printers and Multi-Function Equipment;

(12) ITB-PLT012 – Use of Privately Owned PCs to Access CoPA Resources;

(13) ITB-APP033 – Use of Freeware Policy;

(14) ITB-SEC001 – Enterprise Host Security Software Suite Standards and Policy;

(15) ITB-SEC007 – Minimum Standards for User IDs and Passwords;

(16) ITB-SEC019 – Policy and Procedures for Protecting Commonwealth Electronic Data;

(17) ITB-SEC020 – Encryption Standards for Data at Rest;

(18) ITB-SEC024 – IT Security Incident Reporting Policy; and

(19) ITB-SEC031 – Encryption Standards for Data in Transit.

c. The Commonwealth of Pennsylvania Style Guide:

http://www.portal.state.pa.us/portal/server/pt/gateway/PTARGS_0_2_785_711_0_43/http%3B/pubcontent.state.pa.us/publishedcontent/publish/globel/files/management_directives/management_administrative_support/205_40.pdf

d. Senate Bill 712 of 2005 (Act 94) – Breach of personal Information Notification Act.

http://www.legis.state.pa.us/cfdocs/billinfo/billinro.cfm?syear+2005&sind=0&body=S&type=B&BN=0712

PROCEDURES MANUAL
Commonwealth of Pennsylvania • Department of Corrections

Policy Subject:		Policy Number:
Information Technology		**2.3.1**
Date of Issue:	**Authority:**	**Effective Date:**
November 3, 2015	**Signature on File** **John E. Wetzel**	**November 10, 2015**

Release of Information:

Policy Document: This policy document is public information and may be released upon request.

Procedures Manual: The procedures manual for this policy may be released in its entirety or in part, with the prior approval of the Secretary/designee. Unless prior approval of the Secretary/designee has been obtained, this manual or parts thereof may be released to any Department employee on an as needed basis only.

Section 1 – Responsibilities

Section 2 – Acquisition, Ownership, Installation and Use

Section 3 – Internet Access

Section 4 – Electronic Mail

Section 5 – Document Scanning

Section 6 – Server Room Security

Section 7 – Information Security
(This Section Not for Public Dissemination)

Section 8 – Agency Applications/Systems and their Administration

Section 9 – Offender Use of Computers

Section 10 – Remote Access

Section 11 – Web Content Standards

Section 12 – Institution Offender Internet Access Procedures

Section 1 – Responsibilities

This is a summary of responsibilities related to this Information Technology (IT) policy and procedures manual. They are not intended to be all encompassing.

A. Bureau of Information Technology (BIT)

1. Director

   Serves as the Chief Information Officer (CIO) for the agencies and reports directly to the Department's Executive Deputy Secretary **and** the Office of Administration (OA)/Office of Information Technology (OIT) Deputy CIO for Environment and Public Safety Community of Practice (CoP).

   a. This position is responsible for supplying the agencies with IT, maintaining that IT, and ensuring that the IT continues to support the Agencies' missions.

   b. An organization chart is available on DOCNet located in the IT section under the Bureau/Offices tab.

2. Chief Information Security Officer (CISO)

   The individual responsible for: strategic planning, policy formulation, implementation, ongoing security of all information systems, and data communications programs supported by the BIT. These responsibilities may be delegated to the Information Security Administrator (ISA) by the CISO or CIO, through the title CISO will be used throughout this document.

3. Chief of Applications

   This position is responsible for the development and maintenance of the agencies' applications and databases; and for the enforcement of the Change Management Methodology.

   a. Detailed procedures and guidelines for software engineering are documented in the **DOC Software Engineering Process**, which is stored on BIT's shared drive and available to all BIT staff.

   b. Detailed procedures and guidelines for managing application changes are documented in the **DOC Configuration Change Management Methodology**, which is stored on BIT's shared drive and available to all BIT staff.

   c. Detailed procedures and guidelines for IT service requests are documented in the **BIT Service Request** on DOCNet located in the IT section under the Bureaus/Offices tab.

Issued: 4/4/2012
Effective:4/11/2012

4. Chief of Enterprise Systems

   This individual is responsible for Project Management, Field Services, and the IT budget; and for the enforcement of the Project Management Methodology, and for maintaining Department policy **2.3.1, "Information Technology."**

   a. Detailed procedures and guidelines for project management are documented in the **Project Management General Instructions**, which are stored on BIT's shared drive and available to all BIT staff.

   b. Field Services Section – Oversees the operation of the centralized Help Desk and provides direction to the Business Managers and Facility Information Technology Staff (FITS) related to IT support. Procedures for resolving issues and obtaining services are documented on DOCNet (click on the **Help Desk** link).

   c. Detailed procedures and guidelines for the BIT's budget process are documented in the **IT Budget Process, IT Strategic Plan and CoP** on DOCNet located in the IT section under the Bureaus/Offices tab.

   d. Detailed procedures and guidelines for the IT procurement are documented in the **BIT Procurement Procedures** on DOCNet located in the IT section under the Bureaus/Offices tab.

5. Chief Technology Officer (CTO) or ISA (in the absence of a CISO) – Is responsible for establishing and managing the technical architecture and infrastructure for the Agencies. This individual:

   a. directs the operation of the Agencies' data centers and the disaster recovery site;

   b. manages standards, policies and procedures regarding the organizations IT infrastructure consistent with Commonwealth standards;

   c. establishes and maintains the Agencies' IT infrastructure; and

   d. specifies, technically approves, procures, and manages infrastructure desktop, server, storage, and networking hardware and software.

6. Technical Review Committee (TRC)

   This ***committee*** supports the effective and efficient delivery of BIT services, equipment, and allocation of resources. The TRC must evaluate and approve all such requests. The charter is documented in the **TRC Charter** on DOCNet located in the IT section under the Bureaus/Offices tab.

Issued: 4/4/2012
Effective:4/11/2012

7. IT Governance Committees (ITGC)

   BIT is responsible for conducting ITGC meetings at both the Department and Pennsylvania Board of Probation and Parole (PBPP), with the primary objective to identify, understand, evaluate, and prioritize projects within the IT Project Portfolio. The organization and process are documented in **Department and PBPP IT Governance Organization and Guiding Principles** on DOCNet located in the IT section under the Bureaus/Offices tab.

8. BIT provides a set of services to the agencies. In all cases there is a formal procedure for requesting the service and an established methodology for prioritizing and assigning the work to BIT. Refer to the **BIT Services Inventory** on DOCNet, for a list of the services and how to request them.

B. Central Office Responsibilities – Non BIT Staff

1. Deputy or Agency Head:

   a. makes the formal request to the OA regarding the misuse of E-mail;

   b. makes the formal request to the ***Department's*** Office of Special Investigations and Intelligence (OSII) ***or PBPP Office of Professional Responsibility (OPR)*** regarding misuse of other IT services or Agency information;

   c. serves the agency and BIT by making decisions on matters of high importance or sensitivity, or that are outside of the normal practice for that agency or BIT;

   d. participates in the IT Governance Process; and

   e. approves requests for scanning documents ***(DOC only)***.

2. Bureau and Office Head:

   a. ensures that this policy is adhered to within his/her area of responsibility (i.e. his/her bureau, office or division, etc.) and within his/her business area (i.e., field offices for which they have oversight);

   b. assigns members of his/her staff as Application Administrators to applications or systems that support the business functions within his/her area(s) of responsibility;

   c. notifies the BIT Chief of Applications when changes are required to the Application Administrators;

   d. acts as the interim Application Administrator until a permanent assignment is made; and

   e. participates in the IT Governance process.

3. Application Administrators

   At a minimum, the responsibilities of application administrators, with respect to their assigned applications and/or systems are:

   a. determine and grant (if the capability exists) end user access right;

   b. arrange for, and provide training to, end-users on how to use their application/systems;

   c. answer questions from end users on how to use their assigned application/system in the completion of the end users' job functions;

   d. Analyze changes in policy/law to assess impact on how their application/system is used;

   e. organize a group of subject matter experts (SME's) that are routinely asked for input and perform application /system testing;

   f. recommend new functionality and approve enhancements that support their business area(s);

   g. serve as sole point of contact for BIT service requests;

   h. give final signatory approval for each step in the development of a new application/system, or for enhancements; this includes the final sign-off for acceptance prior to "go-live;" and

   i. designates Local Application Administrators, when the capability exists and this is an appropriate approach to administering their application/system.

4. PBPP IT Liaison:

   a. acts as the single point of contact between BIT and PBPP including OVA, SOAB and FETC;

   b. ensures that requests for service and equipment are in keeping with the overall goals and direction;

   c. ensures that BIT plans for service and equipment upgrades/changes are in keeping with the overall goals and direction; and

   d. monitors Memorandum of Understanding (MOU) compliance by regularly reviewing service related issues and outstanding service requests with BIT.

C. Facility Responsibilities

1. Facility Manager – This is the person who has overall responsibility for a particular facility (State Correctional Institution [SCI], Parole Field Office, Community Corrections Center [CCC], etc.):

    a. ensures that this policy is adhered to at his/her facility; and

    b. ensures that the Local Application Administrators (if applicable) are assigned accordingly to the applications and systems that support the business functions of their facility.

2. Business Manager – this is the manager who is responsible for the FITS:

    a. works with the Facility Manager (at the supported facilities), FITS and BIT to ensure that IT is used effectively and in accordance with Commonwealth and the agencies' policies;

    b. uses the Remedy Help Desk system to manage and track user requests and issues, and assigns tickets to FITS as appropriate;

    c. approves requests to dispose of IT equipment and locally acquired software at his/her facility and submitting information as necessary to ensure that equipment dispositions are reported to the BIT;

    d. establishes procedures at supported facilities to ensure that IT items received by the front desk, mailroom or warehouse are delivered to FITS rather than to the person or area that may have placed the order; and

    e. receives IT projects/initiatives from BIT and assigns the work to the FITS.

3. Local IT Staff – For the Central Office locations, this is the BIT Help Desk staff; for the facilities, this is the FITS at that location; and for all other locations, this is the FITS assigned to support that location:

    a. uses the Remedy Help Desk system to manage and track user requests and issues;

    b. provides technical assistance to staff;

    c. installs IT equipment and software for all supported systems and ensures configuration standards have been established, followed and are maintained;

    d. ensures that IT equipment, software and systems are properly maintained;

    e. ensures that equipment locations meet environmental, electrical and security requirements;

Issued: 4/4/2012
Effective:4/11/2012

f. provides information to staff to allow them to acquire and install appropriate replacement supplies such as printer cartridges, diskettes, magnetic tape cartridges, etc.;

g. troubleshoots and resolves equipment/software problems;

h. maintains accurate inventory information regarding IT equipment and software items that must be tracked but do not need to be recorded on the centralized computer inventory as directed by BIT Field Services;

i. works with users who have purchased non-standard IT systems (e.g., HVAC and Security Systems) to ensure that these systems (software and data) are backed-up and recoverable, and that the documentation and maintenance agreements are in place. Note – it is the user's responsibility to work with the vendor;

j. ensures that the original and a back-up copy of all computer programs on supported computers are maintained in secure storage;

k. ensures that data on servers is backed-up and stored off-site, in accordance with the file backup procedures in accordance with **Section 7** of this procedures manual;

l. ensures that CWOPA accounts are provisioned and administered in accordance with this policy and TID instructions (found at http://cr3mossapp01/sites/BIT/default.aspx);

m. maintains user accounts (adding, changing, deleting, unlocking, resetting passwords, inactivating, or deleting/disabling) for systems for which they are responsible in accordance with procedures that have been established for those systems;

n. in concert with TID, ensures anti-virus software and updates, Host Intrusion Protection software, and security related updates are installed and activated where possible on all supported computers and servers; and that all updates are applied according to schedules established by BIT and OA/OIT;

o. reports any instances of virus detection to the CISO in a timely manner;

p. ensures staff and contracts have access to Commonwealth licensed computer anti0virus software in accordance with policy and license agreements;

q. ensures that IT equipment and software is not used by unauthorized people;

r. informs his/her supervisor in cases of suspected misuse of equipment, software or systems, or other violation of policy;

s. assists in determining if equipment or information has been misused or damaged by inmates, staff or others;

t. ensures that, in accordance with current Commonwealth policy and procedures (see **Section 2**) to the extent possible, all data, information, and computer programs have been removed or are made irrecoverable from equipment or media of which are being disposed;

u. reviews all supported IT equipment, software, systems and networks to ensure they are being used in compliance with this policy;

(1) This includes conducting random, unannounced audits to ensure compliance with copyright laws and the Department's computer configuration standards, including use of passwords.

(2) These reviews are to be performed as special audits as well as on an on-going basis as a part of normal equipment maintenance and support.

v. contacts vendors to obtain service under warranty or maintenance contract for failed machines/systems;

w. reviews local acquisition requests to ensure all IT equipment and software are appropriate and are either on the BIT pre-approved list or will submit the acquisition request to TID; and

x. maintains accurate information on the computer inventory in accordance with procedures established by BIT Field Services.

4. FITS – In addition to the responsibilities listed under Local IT Staff:

a. approves the off-site data storage areas;

b. provides disaster recovery;

c. submits information to the Business Manager as necessary to request authorization to dispose of IT equipment and software;

d. submits information as necessary to ensure equipment and software dispositions are reported to the BIT Field Services Section; and

e. maintains records of all equipment and software dispositions.

D. Other Responsibilities

1. Supervisors:

a. ensure that this policy is adhered to within their area of responsibility;

b. control, authorize, and monitor their employees', contractors' and other persons' access to IT equipment, software, and systems within their areas;

(1) supervisors must ensure that processing, storage, and use of data on computer systems is protected within their areas of responsibility; and

(2) protection of IT resources should be based on data confidentiality the information's value to the organization and potential effect on each facility's security.

c. ensure that, within their area of responsibility, only approved IT equipment, software, and systems are used for the conduct of Commonwealth business;

d. ensure their employees receive training in the appropriate use of the computer equipment, software, and systems as needed to properly perform assigned duties;

e. request/justify application access required for employees under their supervision in accordance with **Section 8** of this procedures manual;

f. notify their immediate supervisor of misuse of equipment of software, or other violation of this policy including attempts/suspected attempts of others to obtain their personal passwords; and

g. approve employee use of document passwords;

(1) supervisors are to retain those passwords in the event those documents are needed in the absence of the employee and

(2) supervisors are prohibited from asking for, obtaining or recording employees' Personal Passwords.

2. Staff, Contractors, and Other Authorized Users of Commonwealth Owned/Licensed IT Equipment and Software:

a. comply with all applicable policies and laws regarding IT. This includes copyright laws, licensing agreements, and other legal restrictions regarding the use of software;

b. ensure that all data, information and computer programs have been removed or are made irrecoverable from media being disposed of, and that data, information and computer programs are destroyed or disposed of only with proper authorization;

c. notify their immediate supervisor of misuse of equipment or software or other violation of this policy including attempts/suspected attempts of others to obtain their personal passwords;

d. report problems and issues with IT to their supervisor or local IT staff;

e. supervise and monitor inmate access to IT equipment, software and systems within their area; this includes:

(1) implementing and monitoring the appropriate safeguards to ensure computers with communication capabilities to which inmates have access are restricted from unapproved access to other computer systems; and

(2) ensuring that inmates are permitted access only to machines that have been designated and marked as inmate-use computers.

f. maintain the security and integrity of their computer passwords by:

(1) not providing or making their password accessible to others;

(2) not allowing others to access systems or perform work under their password;

(3) changing their password on a regular basis; and

(4) immediately changing their password under circumstances where the security of their password has been (or is suspected of being) compromised.

g. adhere to all relevant OA/OIT policies and directives in accordance with **Section 9** of this procedures manual;

h. use the IT hardware, applications, systems, and information for business purposes only; and

i. report to their immediate supervisor any application or system access that is no longer required to perform their job duties.

3. Purchasing Offices shall enforce the procurement rules related to IT procurements.

4. Agency Human Resource Offices and Department Security Office

Based upon the procedures described below, paper forms may need to be stored to demonstrate that the users' acknowledgement of policy.

5. Department Chief Counsel's Office

Review contracts, license agreements, and other types of agreements to ensure that the contracts and agreements do not violate any Commonwealth laws, are in line with the Commonwealth's current standard for IT Terms and Conditions, and at a minimum, protect the Commonwealth's and Agencies' interests. Approve requests for scanning documents.

6. ***Agencies'*** Chief Counsel's Office:

Review contracts, license agreements, and other types of agreements to ensure that the contracts and agreements do not violate any Commonwealth laws, are in

line with the Commonwealth's current standard for IT Terms and Conditions and at a minimum, protect the Commonwealth's and Agencies' interests.

7. IT Administrators – as defined by **Management Directive (MD) 245.18**

   a. Database Administrator – A person responsible for the design and management of one or more databases and for the evaluation, selection and implementation of database management systems.

   b. Network Administrator – A person who manages a communications network within an organization. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program and providing for routine backups.

   c. System Administrator – A person who manages the computer systems in an organization. The responsibilities of a system administrator and network administrator often overlap. A system administrator is involved with operating system and hardware installations and configurations and may be involved with application installations and upgrades. A system administrator may also perform systems programmer activities.

E. Acknowledgment of Policy

1. All persons, except inmates, who use IT equipment, software, or systems supported by BIT, must complete **E-LMS Course MD 205.34 – IT Acceptable Use Policy Review & Acknowledgement (813046md20534-0357).**

   NOTE: If access to the E-LMS system is not available, **MD 205.34, Commonwealth of Pennsylvania Information technology Acceptable Use Policy**, must be read and the appropriate enclosure must be signed. The signed form will be maintained as follows:

   (1) for Agency employees, the form shall be filed by Human Resources in the employee's Official Personnel folder; and

   (2) for non-employees working for the Department, the form shall be filed in the Department's Security Office.

2. All persons who are IT Administrators, as defined by **MD 245.18, IT Administrator Acceptable Use, Auditing and Monitoring, Incident Notification, and Response Policies and Procedures Agreement**, must acknowledge **MD 205.34** and complete the **E-LMS Course MD 245.18**.

3. All persons requiring the use of Remote Access/Control Software must acknowledge **MD 245.18** and complete the **E-LMS Course Remote Access/Control Software Acceptable Use Agreement**.

F. Violation of Policy

1. Violations of the IT Policy or the requirements of this Procedures Manual, including but not limited to the improper acquisition, installation, use, maintenance or disposal of IT equipment of software or the allowance of others to access systems or data without authorization can result in disciplinary action up to and including termination.

2. Additionally, any person who illegally reproduces software can be subject to civil and criminal penalties including fines and imprisonment. The agencies and Commonwealth do not condone illegal copying of software under any circumstance. Making, using or otherwise acquiring unauthorized software can result in disciplinary action up to and including termination.

Section 2 – Acquisition, Ownership, Installation and Use

A. Acquisition

1. Before any Information Technology (IT) acquisition can take place, the funding must be made available through the budget process and Agency approvals are necessary.

    a. Detailed procedures and guidelines for the Bureau of Information Technology's (BIT) budget process are documented in the **IT Strategic Planning, Public Safety Community of Practice (CoP), and Budget Process** on DOCNet located in the IT section under the Bureaus/Offices tab.

    b. Detailed procedures and guidelines for the IT procurement are documented in the **BIT Procurement Procedures** on DOCNet located in the IT section under the Bureaus/Offices tab.

2. Acquisition, installation, maintenance, and disposition of IT equipment and software anywhere within the Agencies, must be pre-approved by the BIT regardless of purpose, funding source or acquisition method, including leasing using the **IT Acquisition Approval Request form** on DOCNet.

    a. This includes General Fund items as well as items procured with grant, manufacturing (Correctional Industries [CI]), Inmate General Welfare Fund (IGWF), inmate organizations or other special funds.

    b. It also includes items offered as donations or surplus, whether through individuals, groups or other government agencies.

        NOTE: For the Department, this is covered in Department policy **3.1.1, "Fiscal Administration."**

3. IT equipment and software acquired with non-government funds, such as inmate organization funds, must be donated to the Commonwealth as a condition of their approval for delivery to, and use in, an Agency; at which time, such items shall be subject to all aspects of this policy.

4. Acquisition, installation, maintenance and disposition of printer, copier, fax and scanner equipment must be in accordance with Office of Administration (OA) IT Bulletins (ITBs):

    a. **ITB-SYM009 - Commonwealth of Pennsylvania Data Cleansing Policy.**

    b. **ITB-PLT010 - CoPA Policy for the Management of Networked Printers and Multi-Function Equipment**.

5. Each facility, Regional Office, and Central Office Bureau or Office may identify areas where there is a need for IT equipment/software, and seek to acquire it in accordance with this policy and funding availability.

Issued: 4/4/2012
Effective: 4/11/2012

B. Ownership

1. IT equipment and software used by staff or inmates for the conduct of Agency functions must be owned, contracted, leased, or licensed by/to the Agency or Commonwealth.

2. All laws and regulations concerning copyrights must be followed.

    a. Copying and/or transmitting documents, software, or other information in violation of copyright laws or license agreements, is illegal and prohibited. This includes copying Commonwealth procured software for use on other equipment at work, at home or elsewhere, as well as copying other software and using it on Commonwealth owned/leased equipment.

    b. Legitimate, approved software shall be provided to all employees who have a demonstrated need.

    c. Software must only be used in accordance with the license agreements.

    d. Use of public domain software (including “open source”, “freeware” and “shareware”) on Commonwealth owned equipment is prohibited unless prior written approval is obtained from BIT and OA/Office of Information Technology (OIT); the applicable ITB’s are:

        (1) **ITB-APP020 - Open Source Software**; and

        (2) **ITB-APP033 - Use of Freeware Policy**.

3. Facility IT Staff (FITS) and BIT must maintain a copy of software licenses, orders, and/or other proof of ownership for software they have acquired to ensure copyright laws are not violated, and keep an automated inventory record to track these licenses for audit purposes.

C. Installation

1. All newly acquired software is to be delivered to the Local IT Staff for holding until installation.

2. For newly acquired equipment, the Local IT Staff is to be notified and shall determine where the equipment is to be delivered and stored.

3. Only persons authorized by BIT may install, download, configure, and remove software from IT equipment owned, leased or acquired by the Agencies.

4. Only software licensed to the Commonwealth or one of the Agencies, and approved by BIT, may be installed on machines owned, leased or acquired by the Agencies.

Issued: 4/4/2012
Effective: 4/11/2012

a. This applies to software acquired from any source, including downloading from the Internet.

b. Personally owned software may not be installed on IT equipment owned, leased or acquired by the Agencies.

c. Personally owned reference materials and information may not be loaded onto or accessed through these machines.

d. Use of screensavers, animated characters, or similar screen displays, other than those provided with approved operating systems, is prohibited.

e. Installation or use of software for amusement (i.e., games) is prohibited except as part of an approved education course.

f. All software which is unlicensed, illegally copied, or unauthorized must be removed from those machines.

g. It is not the responsibility of Local IT Staff or BIT to investigate potential misuse of IT resources (to include the storage of inappropriate files), however:

(1) It is the responsibility of the Local IT staff and BIT to ensure that only approved software is installed on each desktop, and that they are properly updated/patched.

(2) In the normal course of conducting their assigned duties, if they witness any misuse they are to report violations to their supervisor to determine appropriate action.

5. BIT may require that equipment or software acquired without proper approval be un-installed.

6. Software, reference materials, and information may be temporarily installed by BIT approved persons for demonstration/review purposes, as permitted by license agreements. The software, etc. must be removed immediately following the demonstration or specified review period.

7. Only persons authorized by the BIT may install, modify, repair or remove from service IT equipment owned, leased or licensed by/to the Agencies.

8. All Agency owned IT equipment must be recorded on the computer inventory.

   NOTE: The Local IT Staff must ensure that accurate information (especially the serial number and current location) is recorded and kept up-to-date.

9. Except in emergencies, all equipment relocations must have prior approval of the Local IT Staff or BIT.

10. BIT shall have the authority to direct relocation of Agency owned/leased IT equipment and software within and between the Agencies' facilities as necessary to ensure appropriate utilization.

    a. Relocations shall be performed with appropriate notice to affected Facility Managers (or designated points of contact) and/or Central Office heads.

    b. All relocations must be performed in accordance with license agreements and equipment contracts.

    c. The funding source must be considered when reallocating equipment and licenses – BIT will work with the administrator of that area to ensure that proper procedures are followed.

    d. The computer inventory must be updated to reflect the move by the Local IT Staff (for intra-facility moves) or the Field Services Section (for inter-facility moves), in a timely manner.

11. IT equipment is sensitive to various environmental factors. Commonwealth owned/leased equipment must be operated within ranges recommended by the manufacturer.

    a. If not known, a temperature range of 50º-85º Fahrenheit, and a humidity range of 20% to 80% (non-condensing) should be used.

    b. If these parameters are exceeded, BIT must be consulted to determine if use can continue.

12. To the extent practical, IT equipment is to be kept away from direct sunlight, radiators, portable heaters, heating/cooling vents, open windows, and other sources of heat, dust and moisture.

13. The IT equipment area is to be kept free of excessive dirt and dust accumulation, food particles and drink spillage. IT equipment shall not be placed directly on the floor.

14. IT equipment must not be connected to electrical circuits that also supply power to electrical devices that consume electricity in a large, sporadic manner such as air conditioners, heaters, electric motors, and other electrical appliances. Where necessary, UPS (Uninterruptible Power Supply) systems or electrical surge suppressors must be used.

15. IT staff must perform replacement, upgrade, or repair of IT equipment in accordance with **ITB-PLT001 - Desktop and Laptop Technology Standards** and **ITB-SYM009**. Additionally, to ensure all confidential information has been removed, the original hard drives of any IT equipment must be completely erased (wiped) using one of the appropriate methods described in the referenced policies in all cases where the equipment is:

a. leaving the Agencies (including being surplused or transferred to another agency or otherwise taken out of commission);

b. being re-imaged for any reason;

c. being transferred from staff to inmate use;

d. being transferred from one organizational unit to another;

e. being transferred from a staff member who has dealt with sensitive information (such as personnel information or medical information) to a staff member in another area; or

f. being returned to service after being released as the object of an investigation.

16. Though IT staff are involved with the installation of printers, multi-function devices, and (to a limited extent) networked copiers, end-users must:

    a. order and replace expendable supplies such as inkjet and toner cartridges, ribbons, paper, etc.;

    b. perform immediate remediation tasks such as clearing paper jams; and

    c. local IT staff are to assist users when they have questions about the equipment or cannot resolve the issues.

D. Use

1. The computers, servers, operating systems, networks, programs, routines and software installed by the BIT are the property of, are leased by, or licensed to the Commonwealth. All records of computer use, Internet use and/or E-mail communications (sent, received or stored) conducted on Commonwealth IT resources are Commonwealth property and may be reviewed by management at any time in accordance with **Management Directive (MD) 205.34, Commonwealth of Pennsylvania IT Acceptable Use Policy**.

2. All data and records, including those pertaining to computer use, Internet use, e-mail communication, voicemail communication, text messages and other electronic communication sent, received or stored on Commonwealth IT resources are presumed to be the property of the Commonwealth in accordance with **MD 205.34**.

3. All files, data or records stored on, or accessed through IT resources, and all electronic communication and access to Commonwealth IT resources may be searched, traced, audited and/or monitored, with or without notice to the user—including but not limited to all files stored on Commonwealth computers, Internet activities, Internet website access, e-mail, voicemail and text messages in accordance with **MD 205.34**.

4. Employees may not attempt to access data or programs for which they do not have authorization or explicit consent and must keep passwords secure and not share them with others in accordance with **MD 205.34**

5. The Agencies have the right to seize and search any computer, server, storage media, or other IT device at any time. The Agencies may search, access, retrieve, and review files, data or records which are stored on or accessed through its IT resources, as well as records related to the use of IT resources, including Internet records and e-mail communications in accordance with **MD 205.34**:

    a. this above is the responsibility of each Agency's Security, Office of Special Investigations & Intelligence (OSII), or OPR staff – not Local IT Staff or BIT; and

    b. local IT Staff and BIT will assist as requested, but are not equipped or trained to perform computer forensic work.

6. Staff access to IT equipment and software may be suspended or terminated by Agency management at any time with or without cause or notice.

    a. BIT and/or Local IT Staff will assist in implementing this decision, but the decision is management's responsibility – not IT.

    b. Personal information or messages, etc. are not to be entered onto, received, viewed or stored on Commonwealth IT equipment or portable storage media, except as may be approved in accordance with **Section 4 – Electronic Mail** of this procedures manual.

    c. Staff has no rights with regard to access or recovery of data, information or messages stored on the Commonwealth's IT equipment/portable storage media or of any programs, routines, software, etc. developed, installed or stored on this equipment or media.

7. Any suspected misuse of IT resources must be reported through the chain of command to the Bureau/Office Head or Facility Manager:

    a. the Bureau/Office Head or Facility Manager will contact the CIO to report their concerns and request assistance;

    b. the CIO will provide direction based upon the nature of the misuse;

    c. the CIO will direct IT staff as needed to supply the necessary information or resources to the proper investigating authorities; and

    d. in the absence of the CIO, one of the CIO's direct reports will substitute for the CIO.

8. Information Technology (IT) equipment and software owned, leased and/or licensed by the Agencies or Commonwealth must be used only for Commonwealth related and

approved business except as may be approved in accordance with **Section 4 – Electronic Mail** of this procedures manual.

NOTE: It is prohibited for anyone to access or attempt to access the computer programs, software or data stored on this equipment, except as needed to perform assigned duties.

9. Without regard to the method of access or equipment used, it is prohibited for anyone to access or attempt to access the Commonwealth's restricted data or applications (e.g., JNET) except as authorized and as needed to perform assigned duties.

10. Service calls for copiers and stand-alone faxes are the responsibility of the user area, unless there is a technical issue concerning network connectivity that needs to be addressed by the Local IT Staff, and/or, if the unit is being replaced.

11. Agency owned/leased portable IT equipment, such as laptop computers, may be used by employees at home or other off-site locations with the approval of their Bureau/Office Head or Facility Manager:

    a. use of this equipment and software is restricted to Commonwealth business except as approved in accordance with **Section 4 - Electronic Mail** of this procedures manual.

    b. no other use or alterations, including use of games or loading of software or computer programs, is to be performed except as allowed under other sections of this policy; and

    c. the computer inventory will reflect the person/area assigned the equipment.

12. Staff may use approved software (limited to MS Word, Excel, and Access) to develop non-critical standalone computer applications solely for their own use in conducting Commonwealth related business in accordance with **ITB-INF001 - Database Management Systems**. Note that **ITB-INF001** limits the use of this software as these types of applications are difficult to support and are not to be used to support critical business functions. Use of Microsoft Access Databases and other desktop databases to develop stand-alone applications is discouraged. Microsoft Access is suitable as a front-end reporting tool when the report users are limited to a small group or division, but Access shall not be used as an enterprise reporting tool or a shared interface to enterprise database solutions. Access shall not to be used for enterprise or multi-user applications.

13. Distributing applications to other staff is prohibited unless approved by the BIT Chief of Applications and Chief of Enterprise Systems.

14. All applications developed with Commonwealth owned or leased equipment or software, by Commonwealth staff, for Commonwealth use, or on Commonwealth time, are the property of the Commonwealth in accordance with **Management Directive 204.34, Commonwealth of Pennsylvania IT Acceptable Use Policy**.

15. Only staff and contractors authorized by BIT Chief of Applications and Chief of Enterprise Systems may develop computer applications, in accordance with **ITB-APP011 - Application Development Languages** that:

    a. are critical to the Commonwealth business;

    b. use software other than what is approved for staff (limited to MS Word, Excel, and Access);
    c. require complex macro or visual basic coding; or

    d. require programming/analytical support.

16. The development, enhancement, use, and administration of Agency applications are covered in **Section 10** of this procedures manual.

17. An inmate may develop computer applications only within an approved education course and these applications may not be used to record, store, manipulate, display, print or transmit data used by the Agencies – i.e. conduct Commonwealth Business in accordance with **Section 11** of this procedures manual.

18. Staff using networked computers must store all data on the assigned server unless otherwise approved by the BIT.

    a. even classified or confidential data is to be stored on network servers;

    b. local IT staff are responsible for ensuring all servers are backed-up on a prescribed schedule and in accordance with established procedures, including off-site storage of the back-up media as described in the next paragraph; and

    c. FITS must also ensure that a disaster recovery plan for servers is in place and maintained up-to-date.

19. Storage of data on <u>local</u> computer drives for non-networked computers that support functions not supported by BIT, such as HVAC or security, is authorized but the data must be unclassified and must be backed up on a routine/scheduled basis.

E. Standardization

1. IT staff must keep all server and desktop computers up-to-date with service packs and security patches as specified in **ITB-SYM006 – Desktop and Server Software Patching Policy**.

2. BIT and Local IT Staff must follow **ITB-PLT001**.

    a. To the extent practical, IT equipment, software, and systems shall be standardized throughout the Agencies.

b. Standardization will help ensure the following:

(1) that the large amount of equipment and software in the Agencies can be maintained with available resources;

(2) the ability to transfer information throughout Commonwealth government;

(3) continuity of information even when staff changes;

(4) that resources spent on training can be carried with staff as they move to other positions within the Agencies and the Commonwealth;

(5) during an emergency, staff from a variety of facilities will be able to readily access systems and information without need to expend time at critical moments learning new systems; and

(6) an inmate in education programs can maintain a progressive learning pattern when transferred between facilities.

3. Bureaus/Offices having oversight of facility or field functions are to be consulted where appropriate to ensure standardization is considered before acquisition of new computer software is approved.

4. All networks implemented throughout the Department must have prior approval from the Chief Technology Officer (CTO). This approval is based upon the need to address security concerns, the likely need for communication capabilities beyond current application, and for continued support.

5. All network cabling must be installed according to structured cabling standards:

a. this structured cabling standard requires that all network cables be run from the end-user device (PC, printer, other peripheral, etc.) back to a central wiring closet (IDF) that serves the respective building;

b. generally, the central wiring closet for all networks will be the same IDF as is used for the Staff Network;

c. implementation of small, independent networks, dedicated to specific functions is not acceptable;

d. where non-standard networks currently exist, they must be migrated to the standard topology as they are expanded, upgraded or replaced; and

e. any exceptions to this must be approved in writing by the CTO.

6. Any use of existing network infrastructure (routers, switches, cat-5/6 cabling, etc.) requires CTO approval.

   NOTE: Any networks installed for other purposes (e.g., closed circuit television) are not the responsibility of BIT, but may be governed by OA/OIT policies.

7. In accordance with OA/OIT's policies/directives, BIT reserves the right to mandate that certain types of applications be run on thin client terminals instead of personal computer (PC) workstations.

F. Security

1. To prevent unauthorized access, all IT equipment must be secured when staff or other authorized persons are not present:

   a. each person must logoff or password-lock the system/computer when work has been completed or when leaving the general area of the equipment for any reason;

   b. where appropriate, doors to the room(s) in which equipment is located are to be closed and locked when staff or other authorized persons are leaving the area; and

   c. portable media storage devices must also be secured when not in use.

2. Standalone or dial-up access laptop computers must be delivered to the appropriate Local IT staff monthly or in accordance with a schedule established by the BIT Field Services Section so that anti-virus and security related updates can be applied:

   a. when the computer is assigned to an area, the manager of that area is responsible for ensuring this is accomplished; and

   b. when the computer is assigned to an individual, that person is responsible ***for connecting the laptop to the network cable to receive security patches and anti-virus updates***.

3. Any use of a modem within the Agency's facilities must be approved by the Chief Information Security Officer (CISO):

   a. physically connecting a telephone line to a modem that is connected directly to a computer is prohibited if that computer is also physically connected to the Commonwealth's network; and

   b. dial-up modems, whether stand-alone or an internal part of a machine, are prohibited within the secure perimeter of all state correctional facilities except as approved by the Secretary/designee.

4. The screen saver option shall automatically be set by BIT to activate after a period of non-activity; at which point the workstation will be locked and will require a password to unlock it:

    a. in accordance with **ITB-SEC007 - Minimum Standards for User IDs and Passwords**, this is set to 15 minutes, with the exception of workstations located within Department facilities, which are set to five minutes;

    b. this feature must not be disabled by the end-user or Local IT staff; and

    c. any exceptions must be approved by the Technical Review Committee (TRC) and the CIO.

5. Staff may not use software that requires Administrative or Power User rights, except as approved by the BIT CISO.
6. FITS, with the approval of facility management, may install approved security software (e.g., Fortress) on staff and inmate computers to permit/limit these users to only approved functions.

7. IT equipment and portable storage media containing unencrypted “restricted” or “confidential” Commonwealth information may not be checked into airline luggage systems, with hotel porters, or other unsupervised handling or storage processes. Persons should ensure before traveling that the information is either encrypted or that they will be permitted to keep the equipment/media in their possession at all times (such as when taking a commercial airline flight).

8. Inmate-use computers shall be marked by Local IT Staff with the placement of a one inch high red letter "I" on the upper right hand front corner of each monitor and in the upper, center front of each inmate-use CPU. This marking is to be made regardless of how frequently or how much time the machine is used by an inmate. This may be accomplished by using special tags or a permanent marking pen. Also, unless otherwise directed by BIT, special security software must be installed on each inmate-use computer, and it must be configured to permit an inmate to access only approved computer functions.

9. Inmate use computers may not be connected to the Staff Network except as approved by the Facility Manager, CISO, TRC and the Executive Deputy Secretary.

10. Department Central Office, IT (BIT and FITS), and Continuity of Government (CoG) employees are pre-approved to have “all computer access”; all other Department staff (employees and contractors) shall be granted the ability to logon to only one computer required to perform their assigned duties:

    a. assignment of more than their primary PC requires the approval of that staff member’s Facility Manager/Bureau Director and must be justified based on their essential duties and vital to the performance of their job duties;

b. individuals who need to logon to more than fifty specific computers must submit a **FEMM request** for all computer access;

c. the Facility Manager or Central Office Director and their Regional Deputy Secretary shall approve the request prior to final signoff by the Executive Deputy Secretary/Secretary who will indicate the approved time period;

d. all computer access must be tracked by Local IT staff to ensure the user's computer access is "locked down" again at the expiration of the authorization;

e. the BIT CISO shall perform random periodic audits and a 100% audit on an annual basis to ensure all user accounts are "locked down" except those with current authorizations;

f. the ability to logon to all CWOPA computers may be granted without this specific approval where a person is attending a meeting, training, etc. at a non-Department CWOPA site where the specific computer to be used cannot be determined in advance. In these cases, the user's computer access must be "locked down" again immediately following conclusion of the meeting, training, etc.; and

g. access to servers that are not on the standard list (maintained by BIT TID), must be approved by the CISO and CTO.

11. Use of wireless LAN or mobile broadband (WAN) device technology is prohibited anywhere in the Agencies, except as approved in writing by the appropriate Agency Head:

    a. if approved, BIT must adhere to the requirements of **ITB-NET001 - Wireless LAN Technology**;

    b. installation or use of a wireless client network interface card (NIC) or a mobile broadband device in or with an Agency owned or leased PC, Personal Data Assistant (PDA) device or other IT equipment, even if used with other networks, requires this same approval; and

    c. regardless of ownership, wireless interfaces, whether external to or part of another device, are not permitted within the secure perimeter of state correctional facilities, except as approved in writing by the Secretary or Executive Deputy Secretary.

12. Servers and network equipment (i.e., switches, routers, firewalls, etc.) shall be installed in secure and locked locations, with access limited to only authorized staff:

    a. these locations are to be off limits to unescorted inmates;

    b. these locations must meet all necessary environmental requirements; and

c. where servers/network equipment are currently installed in locations that do not meet these requirements, a review should be conducted, plans developed, and steps taken to provide the best security possible until such time as the equipment can be appropriately secured or moved to more secure locations.

13. Storage or recording of inmate, personnel or other confidential information on any digital storage device or media that will be transported off Agency grounds must be encrypted (where the technology allows for it) and have the written approval of the Facility Manager, Bureau/Office Head or higher authority. Employees receiving such approval are responsible for maintaining control of the confidential information and may be subject to discipline if the confidential information is disclosed to a person or organization that is not authorized to receive the confidential information because of the employee's intentional, reckless, or negligent conduct.

14. Contractors must use a Commonwealth approved anti-virus software on computers used to provide files or documents to the Commonwealth, during the tenure of their Commonwealth contract, and may install Commonwealth licensed anti-virus software provided by FITS or BIT in accordance with **ITB-SEC001, Enterprise Host Security Software Suite Standards and Policy**:

    a. in the event this policy changes, the licenses end, the license agreements change, or upon completion or termination of any contracts for such services, contractors must remove all Commonwealth licensed software from the machines on which it was installed; and

    b. though the Local IT Staff may make the anti-virus software available to the contractor, each contractor shall be responsible for installing the software on their computer(s) and obtaining any necessary updates from the software manufacturer's website

        NOTE: Beyond printed installation instructions, Local IT Staff and BIT are not responsible for providing technical support for the installation, updating, or de-installation of this software on personally owned computers.

G. Passwords

1. BIOS/CMOS passwords must follow the standard methodology established by BIT's CISO.

2. Use of Document Passwords is discouraged;

    a. their use is permitted only with the knowledge and approval of an employee's supervisor;

    b. document passwords must be different from the employee's personal password; and

c. document passwords are not confidential and must be provided to the individual's supervisor and any other person who may have legitimate need to access/modify the document(s).

3. Personal Passwords (passwords associated with a person's User-ID) are confidential. Except as noted below, personal passwords are not to be shared or revealed to any other person, including supervisors, Local IT Staff or BIT staff:

   a. in some cases, approved IT staff may need a user's personal password to make modifications to a machine. In these cases only, a user may disclose her/his personal password to that IT staff. However, immediately upon completion of the technical work, the user must change the password. Except for this technical use and for official investigations, it is prohibited for anyone to request, seek, or in any manner attempt to determine the personal password of another person; and

   b. passwords must never be put in an email that also contains the User-ID.

4. Personal passwords must adhere to the following:

   a. must be a minimum of eight characters;
   b. must be composed of at least three of the following types of characters:

      (1) uppercase letters (A.B.C,…);

      (2) lowercase letters (a,b,c,…);

      (3) numbers (0,1,2,3,…,9); and

      (4) special characters (#, other punctuation marks); and

   c. may never contain the user ID, nor any part of the user's full name.

5. In accordance with **ITB-SEC007** log on passwords will expire after 60 days, thus requiring the user to create a new one.

6. Passwords must not be written down and left in a place where unauthorized persons might discover them except for initial password assignment and password-reset situations. If there is reason to believe that a password has been or is suspected of having been disclosed to someone other than the authorized user, the password must be changed immediately.

7. Revealing a password exposes the authorized user to the responsibility for actions that another party takes with the disclosed password. This policy does not prevent the use of default passwords, typically used for new User-ID assignment or password reset situations, which are to be immediately changed when the user next logs into the system.

8. System administrator passwords are to be divulged only to persons approved by the BIT's CISO. System administrator passwords are only to be provided to trained IT employees of the Department and others as approved by BIT's CISO. Temporary or special system administrator passwords may be assigned to computers and divulged to approved contractors by the BIT or Local IT Staff as approved by BIT's CISO to provide those persons the ability to install systems or perform other approved functions. Revised system administrator passwords, approved by BIT's CISO shall be implemented as frequently as necessary to ensure security.

9. Certain computer applications/systems may require assignment and training of an Application Administrator who is required to perform restricted functions such as granting users access, creating backup files, loading or restoring of data from CDs or other media. The BIT CISO must approve such assignments and provision of any passwords. Application Administrators are to be provided the necessary application administrator passwords to allow them to perform the approved functions. Where possible, application administrator passwords are to be separate and different than system administrator passwords used for functions such as configuring and setting the operating system and network configurations. If it is not possible for those two types of passwords to be different, then the password must be changed so it is different than the system administrator passwords generally used on similar equipment.

H. Use of Non-Commonwealth Owned Equipment, Software and Portable Storage Media

1. Personally owned IT equipment and software are prohibited within all Agency facilities except:

   a. approved contractor items used in conjunction with the conduct of functions contracted by that Agency and approved by the affected Facility Manager and BIT CISO; or

   b. equipment and software used in connection with court proceedings.

2. Only equipment, software and portable storage media owned, leased or licensed to the Agencies may be connected to or used with Agency owned/leased IT equipment or systems:

   a. specifically prohibited is connection/use of employee or contracted staff's privately owned equipment, software and portable media storage devices in accordance with **ITB-PLT012 - Use of Privately Owned PCs to Access CoPA Resources**;

   b. this prohibition exists regardless of how that connection is made (via network, direct, cable or wireless connection);

   c. any exception to this must be approved in writing by Executive Deputy Secretary and BIT CISO.

3. Where practical, the Agencies shall provide Agency owned/leased IT equipment and software to contractors for the conduct of business on behalf of the Agencies, if work is being done on CW premises. Where contractors are required to or must utilize IT equipment that they provide for the conduct of work on behalf of the Agencies, the hard drives, and all other media, including portable storage media must be turned over to BIT for destruction at the conclusion of that business. All exceptions to this must be approved in writing by the BIT CISO.

4. IT equipment, software, and networks owned or leased by contractors for use by their employees within the Agencies must be approved by the BIT CTO and CISO.

5. In accordance with **ITB-PLT012**, use of "Public" computers (e.g., computers provided by libraries, universities, coffee shops, hotel business centers, etc. for general public use) to access the CoPA network is prohibited:

   a. use of a public computer to connect to a Commonwealth owned network poses a significant security risk in that a third party may more easily capture a user's logon credentials;

   b. where Commonwealth business must be conducted away from the worksite, Agency owned or leased portable equipment should be provided where possible;

   c. staff must ensure that inmate, personnel or other confidential information is not inadvertently or otherwise moved to non-Agency owned/leased computers or media;

   d. special risks exist and care must be taken where staff access Commonwealth E-mail and systems using non-Agency owned/leased equipment;

   e. this risk is heightened if any part of that equipment is connected to a wireless network;

   f. inmate, personnel or other confidential information, including attachments, shall not be downloaded to equipment where it may become available to unauthorized persons;

   g. staff must be aware that simple deletion or erasure of information on a computer system does not eliminate the possibility of it being recovered by unauthorized persons; and

   h. transfer of data from Agency owned computers to non-Agency owned/leased computers is prohibited except where specifically approved in writing by a person's immediate supervisor.

I. Portable Media Storage Devices

1. Portable storage media presents a security risk for the Commonwealth and the Agencies, both because of the ability to transfer large amounts of data and the potential for inmates to obtain and misuse these devices. Additionally, the Agencies must ensure that inmate,

personnel, and other confidential information/documents are protected from unauthorized disclosure.

2. Only Commonwealth owned portable media storage devices are to be used with Agency owned/leased equipment:

   a. any exception to this must be approved in writing by the BIT CISO; and

   b. use of privately owned media & devices is specifically prohibited.

3. Personal portable media storage devices are prohibited in all Agencies' Facilities.

4. Portable media storage devices are not to be used by end users for storing Commonwealth data, except as approved by the BIT CISO, or as permitted elsewhere in this policy.

5. All portable media storage devices used with Agency owned/leased computers, or with contractor owned computers on behalf of the Commonwealth, are to be turned over to FITS or BIT Help Desk for transfer to the Department of General Services (DGS) for disposal when no longer needed.

6. All devices capable of writing to any portable media storage device and all portable media storage, except floppy disks, CDs, DVDs and magnetic tapes:

   a. must have their acquisition and intended use approved by both the BIT CISO, and the Facility Manager or Bureau/Office Head on a case-by-case basis;

   b. must be recorded and tracked by the Local IT staff on an inventory as approved by the BIT CISO;

   c. must be inventoried by the Local IT staff at least twice a year;

   d. are prohibited within the secure perimeter of facilities, except as approved by the Facility Manager;

   e. may only be used by a limited number of people as approved by the Facility Manager or Bureau/Office Head;

   f. must utilize password protection and encryption (where possible) on media being transported off Agency grounds when being used to record inmate, personnel or other confidential information;

   g. must not be used for data backup procedures; and

   h. must not be used for data retention in excess of seven days (does not apply to media used exclusively with digital cameras).

7. At Department facilities, Local IT Staff must provide information/training to security staff so they can recognize portable storage media to prevent unapproved introduction into facilities.

8. CDs/DVDs in a DOC Facility:

   a. a formal system of accountability must be established for all CDs/DVDs when inside the secure perimeter of a Department facility;

   b. procedures shall be established to secure and account for CDs/DVDs when inside the secure perimeter of a Department facility; and

   c. any missing media must be reported immediately in accordance with local procedure.

9. CDs/DVDs shall be used to store data as part of an established back-up routine for PCs that are not connected to a network which do not have any other approved method of back-up available.

J. Disposition of Equipment and Software

1. All equipment must be checked by IT staff prior to replacement or disposal to ensure that any hard drives are appropriately cleansed of data and are handled in accordance with **ITB-SYM009**, this includes:

   a. computer system and multifunction fax/print/scanner hard drives, removable media, and hand-held devices;

   b. hard drives replaced as part of a repair or maintenance process; and

   c. all computer equipment used by contractors to perform work for the Commonwealth when the contractor has completed his/her engagement.

2. To the extent possible within copyright laws, removal of unlicensed, illegal or unauthorized software is to be accomplished in a manner that will retain needed information and not disrupt normal business functions. Also, where practical, supervisors are to be informed of the intended removal of software, systems or data from their areas.

3. All IT equipment and software must be disposed of in accordance with Commonwealth policy. All IT equipment dispositions require BIT approval which may be provided by pre-approval to surplus specific types, makes, models, classes or conditions of equipment or in response to requests regarding other specific items.

4. Business Managers must approve requests to dispose of IT equipment and locally acquired software at their facilities and supported facilities. FITS must maintain records of all IT equipment and software dispositions.

5. All IT equipment dispositions must be handled in accordance with direction from the Department of General Services, which shall determine the appropriate method of disposal.

K. Electronic Records Management

1. **MD 210.9, The Commonwealth's Enterprise Records Management Program**, establishes policy, responsibilities and procedures for the management of records, including electronic records. Staff are to refer to that policy with respect to the creation, use, maintenance, scheduling and disposition of electronic records.

2. Staff are to conform to Enterprise Records Management specified retention periods and disposition for computer system backup tapes and computer system log files.

L. Remote Access/Control Software Acceptable Use

Certain IT staff require the use of Remote Access/Control Software to remotely access Commonwealth IT resources.

1. Only It staff (BIT staff, FITS, IT Contractors, and any specific NON-IT individual given special approval by the CISO); are permitted to use this type of software on Commonwealth IT resources.

2. IT staff are trusted with rights and privileges beyond those granted to a normal Agency user and therefore must adhere to the highest standards of conduct while using REMOTE ACCESS/CONTROL SOFTWARE when providing support.

3. Applicable policy acknowledgement is required before use in accordance with **Section 1** of this procedures manual.

4. No other individuals are allowed to use this type of software on Commonwealth IT resources.

5. This software usually requires that the IT staff using it have Administrative Rights.

6. It staff must inform and receive a user's approval prior to using this software to remotely access that user's computer.

7. It staff must ask and receive confirmation from the user that there are no restricted applications currently running on the PC or confidential data displayed on the user's screen, before initiating such remote access session.

8. Any confidential information accessed or viewed by IT staff must not be disseminated or disclosed to anyone.

Section 3 – Internet Access

A. Internet Access

1. Internet access will be available from end user devices as listed below:

    a. Staff end user devices that connect to Commonwealth of Pennsylvania (COPA) information technology (IT) resources (i.e. devices requiring CWOPA login credentials). This internet access will be provided through the COPA's internet service provider (ISP) via COPA IT resources.

    b. Offender end user devices that connect to Department of Corrections (DOC) institution inmate-network resources. This internet service will be provided through COPA's ISP via COPA IT resources.

    c. Offender end user devices that connect to Community Corrections Center (CCC) or Community Contract Facility (CCF) non-COPA IT resources. This internet service will be provided through the ISP contracted by the CCC or CCF.

B. Internet Web Site Accessibility

1. Internet access filtering systems and/or firewall rules will be used to regulate internet sites accessible by the various end users.

2. COPA internet filtering systems will be used for staff end user devices that connect to COPA IT resources.

    a. Internet access levels will be established to govern the web site categories accessible by staff end users. The **Internet Access Levels (Attachment 3-A)** identifies the various staff internet access levels and web site categories accessible by each access level.

    b. Staff end users will be assigned to a default internet access level based upon their job classification. The **Job Classification Default Access Levels (Attachment 3-B)** identifies the default access level for each job classification and these access levels will be associated with staff members' CWOPA user IDs. Staff end users will have the same internet access privileges on all Agency devices for which they have IT security privileges.

    c. DOC supervisors may request changes to the default access level for their staff using the Front End Management (FEM) system on DOCNet.

    d. Pennsylvania Board of Probation and Parole (PBPP) supervisors primarily assigned to a work location at a DOC institution may request changes to the default access level for their staff using a **PBPP End User Internet Access Change Request (Attachment 3-C)**.

Issued: 11/3/2015
Effective: 11/10/2015

e. PBPP supervisors not primarily assigned to a work location at a DOC institution may request changes to the default access level for their staff via an email sent to the PBPP Director of Internal Affairs/Specialized Services. The PBPP Director of Internal Affairs/Specialized Services will then forward all approved requests to the Bureau of Information Technology (BIT) Network Communications Section for processing.

f. Staff end user access levels will be associated with the particular staff member's CWOPA user ID and staff end users will have the same internet access privileges on all Agency devices for which they have IT security privileges.

g. Some computers at DOC institutions will have an access level assigned to the machine. The **Devices with Internet Access Applied to the Device (Attachment 3-D)** identifies these devices and the access level associated with each. All staff using these computers will have the access level assigned to the machine. However, the staff member's personal CWOPA-ID-based access level will override the access level assigned to the machine in cases where the individual's access level is higher than the level assigned to the machine. All requests to have specific devices considered for this type of access should be submitted via email through the chain of command to the DOC Executive Deputy Secretary.

3. COPA internet filtering systems will be used for offender end user devices that connect to DOC institution inmate-network resources.

   a. Offender end user devices connected to DOC institution inmate-networks will be classified by the functional purpose of the device (e.g. Transitional Housing Units, Academic Labs, etc.) and the associated internet access privileges will be defined for each unique offender end user device classification. The BIT Network Communications Section will maintain documentation that identifies the various internet classifications and the access privileges associated with each classification.

   b. Access privileges will be associated with specific DOC institution inmate-network computers and all offenders using these computers will have the access privileges assigned to the particular computer.

4. ISP and/or device-based internet filtering technology will be used for offender end user devices at CCCs and CCFs that access the internet via contracted ISP network resources. The filtering systems and configuration rules used to regulate offender internet access at CCCs and CCFs will be defined in Department policy **8.3.1, "Community Corrections Security," Section 28.**

C. Internet Use

1. End users accessing the Internet through Commonwealth IT Resources shall comply with the requirements identified in **Management Directive 205.34, "Commonwealth of Pennsylvania Information Technology Acceptable Use Policy."**

2. The dissemination of information over the internet must adhere to Department policies **DC-ADM 003, "Release of Information;" 1.3.2, "Citizen, Legislative, and Executive Office Inquiries;"** and the **PBPP Procedures Manual, Chapter 1, Section 4, Procedure 4, "Release of Information."**

3. Policies and procedures regarding offender internet use at DOC institutions are defined in Department policy **2.3.1, "Information Technology," Section 12**.

4. Policies and procedures regarding offender internet use at CCCs and CCFs are defined in Department policies **8.3.1, Section 28;** and **BCC-ADM 006, "Residential Services Procedures Manual," Section 1**.

D. Responsibilities

1. Executive Deputy Secretary shall:

   a. approve all staff internet access levels as defined in the **Internet Access Levels**;

   b. approve all default internet access levels for job classifications as defined in the **Job Classification Default Access Levels**;

   c. review and approve all requests for DOC device-level internet access classifications as defined in the **Devices with Internet Access Applied to the Device**; and

   d. approve all DOC institution offender internet device classifications and access privileges.

2. PBPP Director of Internal Affairs/Specialized Services shall:

   a. make recommendations regarding the PBPP staff internet access levels defined in the **Internet Access Levels**;

   b. make recommendations regarding the default internet access levels for PBPP job classifications defined in the **Job Classification Default Access Levels**; and

   c. approve all changes to the default internet access levels assigned to PBPP staff.

3. BIT shall:

   a. make recommendations regarding the DOC staff internet access levels defined in the **Internet Access Levels***;*

   b. make recommendations regarding the default internet access levels for DOC job classifications defined in the **Job Classification Default Access Levels**;

   c. make recommendations regarding the device-level internet access classifications defined in the **Devices with Internet Access Applied to the Device**;

d. make recommendations regarding the DOC institution offender Internet device classifications and access privileges and document those recommendations that are ultimately approved;

e. establish configurations standards for the staff and institution offender end user devices to be used to access the internet through Commonwealth IT resources;

f. design, implement, and support the IT infrastructure required to meet the requirements set forth in this policy;

g. administer the COPA Internet filtering systems;

h. configure the central office staff end user devices to be used to access the internet;

i. provide 1st and 2nd level technical support for staff internet access and DOC institution offender internet access; and

j. provide technical assistance and make recommendations to Bureau of Community Corrections (BCC) staff regarding the configuration of offender devices and the internet filtering systems used at CCCs and CCFs.

4. BCC shall establish Department policies and procedures regarding the acquisition, use, administration, and support of offender internet access at CCCs and CCFs.

5. Central Office Director/Facility Manager shall:

   a. process all requests for changes to staff internet access levels;

   b. supervise staff end user internet access to ensure compliance with Department policy; and

   c. supervise offender internet access at DOC institutions to ensure compliance with Department policy.

6. Facility IT Staff shall:

   a. configure, install, and maintain staff and institution offender end user devices in accordance with BIT direction and standards;

   b. provide 1st level technical support for staff end user internet access; and

   c. provide technical assistance to other staff supporting offender end user internet access.

7. Unit Managers shall supervise offender internet access at DOC housing units to ensure compliance with Department policy.

8. Staff Proctors shall provide 1st level assistance for offender end user internet access. Staff Proctors are any staff that supervise offender internet usage.

9. Supervisors shall:

    a. process all requests for changes to staff internet access levels; and

    b. ensure that staff and contract employees are aware of and abide by **Management Directive 205.34, "Commonwealth of Pennsylvania Information Technology Acceptable Use Policy."**

10. Staff End Users shall complete the annual training requirement to review and acknowledge **Management Directive 205.34, "Commonwealth of Pennsylvania Information Technology Acceptable Use Policy."**

E. Applicability

1. "PBPP" as used in the context of this policy applies to the following Boards, Offices, and Commissions:

    a. the Firearms Education and Training Commission;

    b. the Office of the Victim Advocate; and

    c. the Sexual Offender Assessment Board.

2. This policy applies to all employees and contract staff of the following Agencies:

    a. the DOC;

    b. the PBPP;

    c. the Firearms Education and Training Commission;

    d. the Office of the Victim Advocate; and

    e. the Sexual Offender Assessment Board.

Issued: 11/3/2015
Effective: 11/10/2015

Section 4 – Electronic Mail

A. General Usage

1. Electronic Mail (E-mail) may be used only for business related purposes to transmit business information and, with approval of the Facility Manager, for organizations that benefit all employees of a facility.

2. E-mail may not be used for chain letters, jokes, pornography, non-Commonwealth endorsed charitable drives, special interest groups; or to engage in any communications that are in violation of any Agency policy, the Code of Ethics, **Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy** or criminal in nature. The aforementioned items may not be sent to/from an Agency owned computer from/to any other computer, including a home computer.

3. E-mail and the Internet are information tools that the Commonwealth has made available on Commonwealth computer resources for Commonwealth business purposes. However, where the Agencies determine that personal use of these resources does not interfere with the efficiency of operations and is not otherwise in conflict with the interests of the Agency, reasonable use of the Internet and/or E-mail for personal purposes will be permitted in accordance with standards established for business use. Where authorized by the Agencies, such personal use shall be limited, occasional, and incidental. Any personal use which is inconsistent with Commonwealth policy regarding availability or capability of computer equipment, or appropriate content of communications as defined by this policy is not permitted.

4. Employees shall not retain personal E-mails as this impacts network performance.

5. For Department staff only:

    a. For security reasons, only certain staff (employees and contractors) will be granted Unrestricted E-mail. All other staff will be restricted to sending E-mail within the PA state government E-mail system (Commonwealth of Pennsylvania [CWOPA] global address list). Requests for unrestricted E-mail shall be processed using a FEMM request.

    b. A Deputy Secretary and a Facility Manager or Bureau/Office Head must approve all requests for unrestricted E-mail within the secure perimeter of a facility. All other E-mail requests must be approved by a Bureau/Office Head.

B. Confidential Agency Information

1. A greater degree of caution must be exercised when transmitting any information via the E-mail system and must be in accordance with Agency policies concerning release of information in accordance with Department policy **DC-ADM 003, "Release of Information"** or for the Pennsylvania Board of Probation and Parole (PBPP) refer to the procedure Release of Information in the Communications section of the PBPP Operations Manual, as well as any applicable laws (e.g., Criminal History Records

Information Act). The CWOPA E-mail system does not encrypt email messages or their attachments for e-mail sent within the Commonwealth. Use of the "Send Secure" option shall be used to encrypt e-mails sent to e-mail addresses external to the Commonwealth.

2. Care must always be used in addressing E-mail messages to make sure that messages are not inadvertently sent to inside or outside recipients that are not authorized to receive the information. In particular, care must be exercised when using distribution lists to make sure that all addresses are appropriate recipients of the information. Individuals using lists should take measures to ensure that the lists are current.

C. Viewing and Protecting E-Mail

1. All E-mail messages sent, received, or stored on a Department or Commonwealth network is the property of the Commonwealth and may be reviewed and retrieved by management at any time.

2. To guard against dissemination of confidential Agency information, individuals must not access E-mail messages in the presence of others who are not authorized to view this information, and are responsible for ensuring that confidential Agency information is only sent to people who are authorized to view this information. If confidential information is inadvertently sent to an unauthorized person, the employee must immediately notify his/her supervisor and contact the Bureau of Information Technology (BIT) Chief Information Security Officer (CISO) to determine if the information can be recovered before it is viewed.

3. Users who share a workstation must close E-mail when finished working with it and must log off the workstation when they are done working.

4. The Agency head/designee shall determine who has access to review another user's E-mail, which may include executive level staff, legal staff, system administrators, and individuals in the user's chain of command. Access to E-mail maintained on the Commonwealth's central E-mail server shall be in accordance with Office of Administration (OA) policy and procedures including **MD 205.34**.

5. Upon notification that an individual is no longer employed by or performing services for the Commonwealth, Local IT Staff or BIT shall immediately delete that individual's CWOPA account (which includes access to E-mail).

6. Users must not open any E-mail from an unknown source or questionable origin. Security Awareness is essential. Users must follow best security practices regarding E-mail security.

    a. **DELETE the E-mail** in question.

    b. If the E-mail has been opened, **DO NOT REPLY** or **FORWARD** the E-mail, immediately **DELETE the E-mail** in question (reference below section on Reporting SPAM or Not SPAM below).

c. **Do not click** on any links or attachments in questionable E-mails.

d. Never provide any user id's, passwords or personal information (i.e. account numbers, SSN's, birthdates etc.).

7. Reporting SPAM or Not SPAM

a. Users who receive SPAM may request that the sender be blocked from their inbox by forwarding the E-mail to: CWOPA SPAm@state.pa.us prior to deleting the email as instructed above.

b. Users who discover that messages that were quarantined by the Commonwealth as potential junk mail, are actually not SPAM, may request the sender's address be added to their inbox by forwarding an E-mail to: CWOPA NOT spam@state.pa.us.

D. E-mail Etiquette

E-mail messages may be read by someone other than the addressee and may even have to be disclosed to outside parties or a court. Users must ensure that messages are courteous, professional, and businesslike.

E. E-mail Formatting Standards

1. E-mail is to have a plain white background (no colors, borders, designs, animations or other special effects). Except where emphasis is required, regular font style and black or blue colored type should be used.

2. In accordance with the **Commonwealth's Style Guide**, all E-mails sent by Commonwealth employees that work for agencies that fall under the Governor's jurisdiction must use the below E-mail signature:

Employee Name l Employee Position Title
Agency Name
Street Address l City, State ZIP
Phone: 999.999.9999 l Fax: 999.999.9999
EName@state.pa.us
www.agency.state.pa.us

This message is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential, and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient or the employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please immediately notify the sender and then delete the communication from your electronic mail system.

3. All staff (excluding the Office of Chief Counsel) are required to include the confidentiality statement as listed above. The Office of Chief Counsel has a confidentiality statement specific to their line of business.

4. No banners, quotations, photos, etc. are to be included as part of the signature.

F. E-Mail Retention and Disposition

a. **MD 210.5, Records Management**, establishes policy, responsibilities and procedures for the retention and disposition of records, including E-mail. Staff are to refer to that policy with respect to the retention and disposition of records created on E-mail systems.

b. Storage of large numbers of E-mail messages in the Outlook Inbox, Sent Items, Deleted Items and personal file areas is discouraged. Excessive storage of E-mail hampers server speed, file retrieval time and overall performance.

c. E-mails should be retained or disposed of ONLY in accordance with the applicable records retention schedule(s).

d. Users should promptly delete any E-mail messages they send or receive that no longer require action or are not necessary to an ongoing project. Users should audit their stored E-mail messages periodically to identify messages that are no longer needed for Commonwealth business, especially personal messages.

e. Because of the effect it may have on the network, sending large attachments, especially to a large number of persons, is discouraged.

f. The OA sets the standards for the size of user mailboxes on their servers, the maximum allowable size of attachments, etc. and these are subject to change.

Section 5 – Document Scanning

A. Approval for Use of Document Scanning

The following procedures detail the requirements for submitting requests for approval to use document scanning where acquisition or use of scanning equipment, software, data storage or transmission over data lines is required. Approval is required before Information Technology (IT) staff can acquire, install or facilitate the use of document image scanners, including replacements for scanners not previously reviewed.

1. Field requests for use of multifunction devices for "scan-to-email" functionality where scanned documents will not be electronically stored, shall be submitted via an email to the Business Manager for field sites and, for Central Office staff, to the Help Desk via an email. The email must include business justification for the request and must be submitted by a management level staff. **Requests for scan-to-email from multifunction devices which are inside the secured perimeter of a facility must have the approval of the Facility Manager**. All staff granted "scan-to-email" capability shall be responsible and accountable to ensure that scanned documents comply with the Criminal History Records Information Act (CHRIA), security, and/or privacy laws, policy and procedures.

2. Field, facility, or Central Office Bureau staff desiring to implement document scanning other than "scan-to-email" must submit a **Service Request Form** and **Document Scanning Request Form (Attachment 5-A)** (available on DOCNet) to verify that the proposed scanning use meets the requirements of both Agency and Commonwealth policy.

3. Use of document scanning for any purpose within the Agencies requires review and approval by that Agency's Office of Chief Counsel and appropriate Executive Deputy Level Senior Staff. These approvals must be obtained before the acquisition or use of any document scanning hardware or software and before implementing any initiative requiring electronic storage, system processing, or network access of scanned documents or records. The following procedures shall be followed:

    a. Requestor

    Staff requesting to use document scanning where acquisition or use of scanning equipment, software, data storage, or transmission over data lines must submit a **Service Request Form** and the **Document Scanning/Approval Request Form**. The requestor must ensure the forms are complete and accurate.

    b. Facility Manager/Central Office Director

    The Facility Manager or Central Office Director must review the **Service Request Form**, the **Document Scanning/Approval Request Form** and all attachments, and, if in agreement, complete the appropriate section of the **Document Scanning/Approval Request Form**. Both forms and all attachments shall then be forwarded to the Office of Chief Counsel for review.

c. Office of Chief Counsel

(1) The Office of Chief Counsel shall review all forms and attachments, the types of documents to be scanned and managed from a legal/CHRIA perspective in light of proposed use and complete the appropriate section of the **Document Scanning/Approval Request Form**.

(2) All forms and attachments shall then be forwarded to the Bureau of Information Technology (BIT) Technical Review Committee (TRC). Disapproved requests should be returned to the Facility Manager/Central Office Director.

d. BIT Technical Review

BIT will conduct a technical review of the request as follows:

(1) All requests will first be reviewed by the BIT Network Section for technical feasibility, impacts on data networks, and estimates of any out-of-pocket costs required for implementation. The Network Section will record its recommendation on the **Document Scanning/Approval Request Form**.

(2) The request will then be reviewed by the Field Servers Section for storage and backup/archiving impacts and requirements. This staff will also provide any estimates for any out-of-pocket costs for storage, servers, and/or any other hardware or software. The Field Servers Section will record its recommendation on the **Document Scanning/Approval Request Form**.

(3) The request will then be reviewed by the Applications and Database sections of BIT to evaluate any impact on application systems. This staff will also provide any estimates for any out-of-pocket costs for any software acquisition, development, and/or implementation costs. The Applications/Database Section will record its recommendation on the **Document Scanning/Approval Request Form**.

(4) The BIT TRC will review all forms and attachments for technical feasibility and impact on Department or Pennsylvania Board of Probation and Parole (PBPP) technology systems and approve or disapprove the request. Approved requests will be forwarded to the appropriate Department Deputy Secretary or PBPP Senior Executive for final review. Disapproved requests will be returned to the Facility Manager/Central Office Director for return to the submitted.

e. Department Deputy Secretary/PBPP Senior Executive

Review all forms and attachments and, if in agreement, complete the appropriate section of the **Document Scanning Request Form**. All forms and attachments should then be returned to the BIT TRC.

f. BIT TRC

The TRC will review the forms to ensure that all necessary information has been provided and approvals have been granted. If complete, the TRC will then inform facility and/or internal BIT staff that acquisition/use of scanning may proceed. If not complete, the requesting facility/Central Office area will be informed of any deficiencies and provided opportunity to make corrections and provide additional information.

4. Document scanners include both single function devices that can only be used as a scanner and multi-function devices where one of the functions includes document scanning (for example, a device that can be used as a copier, printer and scanner).

5. For the purpose of this policy, document scanners do not include:

   a. bar code scanners such as used to read identification tags or labels on packages and grocery items;

   b. Optical mark Recognition (OMR) scanners (bubble form readers) such as used to grade tests; and/or

   c. other types of scanners whose sole use is to perform or substitute for the same type read and interpretation as bar code or OMR scanners.

B. Scanning Project Requirements

1. Use of scanning equipment creates electronic copies of documents that become records. The creation, use, maintenance, scheduling and disposition of electronic records must comply with **Management Directive (MD) 210.5, The Commonwealth's Enterprise Records Management Program**.

2. Electronic Document Management Systems (EDMS) are usually commercial software systems or specific vendor developed and provided systems. These systems usually involve the scanning of large numbers of specific types or categories of documents and the electronic storage of those documents. EDMS systems are used to manage documents across the document life cycle. Scanned documents may be used as electronic records in place of the original documents. Requirements for the implementation of this type of system are detailed in **Information Technology Bulletin (ITB)-INFRM006 – Electronic Documents Management Systems** and **ITB-INFRM007 – Management of Electronic Information Created via Multi-Functional Devices or Other non-EDMS Desktop Scanners**.

3. For the purpose of this policy, scanners include all desktop document scanners and multifunction scanners.

   a. **ITB-INFRM007** contains the requirements that must be followed for the implementation of multifunction scanners.

b. BIT and/or Facility IT Staff (FITS) are to review types of documents to be scanned, assist with scanner configuration for correct file format output/resolution, and instruct users. The purpose of the instruction is to address issues of quality and image file sizes. The instruction will also encompass the way in which the digital imaging equipment should be used to create, record, transfer, retain and dispose of the digitized images.

c. Scanned images must be retained in accordance with approved records management schedules. The facility/Central Office Bureau/Office using the scanner must contact the Agency's Records Administrator to amend the Agency-Specific Records Retention Schedule to reflect record series amendments/additions. Amendments must allow for electronic versions of records. An analysis must be performed to determine where the scanned versions fit into the scheduling process. Annotations by vendors or staff may make the original scanned versions updates of the originally scanned records. Also, scanned records may be needed as proof of receipt, manufacturing changes, etc.

d. The requesting facility or Central Office Bureau/Office must conduct an analysis, in conjunction with the BIT, to determine:

(1) the impact on the network and infrastructure to include a determination that the network is image-capable and that imaging will not degrade network performance;

(2) how much data will be generated and the current and future data storage capacity requirements. It must be ensured that each scanned document requires only a limited amount of storage; and

(3) that the proposed indexing and retrieval scheme will meet legal and operational requirements.

4. The altering or manipulation of the scanned image from its original format is prohibited for those being maintained as original documents. Scanning applications must be "locked-down" so that image manipulation/alteration is prevented for these documents. Scanning or document management software that permits electronic layers or over-lays for purposes of redaction without modifying the original document are acceptable.

5. Scanners will be defaulted to the Portable Document Format (PDF).

Section 6 – Server Room Security

Servers shall be installed in secure and locked rooms/cabinets, with access limited to only authorized staff.

A. Central Office

1. Physical Security and Environmental Maintenance

    a. Doors to the Central Server Room shall not be left unlocked at any time.

    b. The Bureau of Information Technology (BIT), Technology Infrastructure Division staff shall ensure that all doors to the ***Technology Parkway (TEC)*** Server Room are tightly closed and locked at the end of each work day.

    c. The BIT Technology Infrastructure Division staff ***shall confirm with the Bureau of Operations*** that the Uninterruptible Power Supply (UPS) system and related electrical equipment that serves the ***TEC*** Server Room is maintained by vendors and checked ***routinely*** to confirm it is in good working order and that any necessary repairs are made as quickly as possible.

    d. The BIT Technology Infrastructure Division staff shall ***confirm with the Bureau of Operations that air conditioners serving the TEC*** Server Room are maintained by a vendor and checked ***routinely*** to confirm that they are in good working order and that any necessary repairs are made as quickly as possible.

2. Access to the ***TEC*** Server Room

    a. Only persons with official Commonwealth business shall be permitted access to the ***TEC*** Server Room.

    b. Vendors and other ***non-departmental*** staff shall not be left unattended in the ***TEC*** Server Room without the approval of the BIT's Chief Information Security Officer (CISO) ***or Information Security Administrator (ISA)***.

3. Vendors and Other Non-Departmental Staff

    a. Any vendor and/or other ***non-Departmental*** staff shall be required to sign in and out at the facility reception desk.

    b. Any vendor and/or other ***non-Departmental*** staff needing access to the ***TEC*** Server Room shall be escorted by a Department employee between the reception area and the Server Room on his/her way to and from the room.

    c. Any vendor and/or other ***Non-Departmental*** staff shall not be provided unattended access to any device(s) in the ***TEC*** Server Room and shall not be provided any password(s) that would allow access to production data on that device(s).

Issued: 8/19/2011
Effective: 8/26/2011

B. Facility

1. Physical Security & Environmental Maintenance

    a. Doors to a facility server room shall not be left unlocked at any time.

    b. Facility IT Staff (FITS) shall ensure that all doors to the facility's server room are tightly closed and locked at the end of each workday.

    c. FITS shall ensure that the UPS systems and related electrical equipment that serves the facility server room is checked quarterly to confirm that they are in good working order and that any necessary repairs are made as quickly as possible.

    d. FITS shall ensure that air conditions serving the facility server room are checked quarterly to confirm that they are in good working order and that any necessary repairs are made as quickly as possible.

2. Access to the Facility Server Room

    a. Only a person with official Commonwealth business shall be permitted access to the facility server room.

    b. A vendor and/or other ***non-Department*** staff shall not be left unattended in the server room.

3. Vendors and Other Non-Departmental Staff

    a. Any vendor(s) and/or other ***non-Department*** staff must sign the server room registration book upon entering and exiting the room.

    b. Any vendor(s) and/or other ***non-Department*** staff shall not be provided unattended access to any device(s) in the server room and shall not be provided any password(s) that would allow access to production data on that device(s).

Issued: 8/19/2011
Effective: 8/26/2011

CONFIDENTIAL

2.3.1, Information Technology

Section 7 – Information Security

This section is confidential and not for public dissemination.

Section 8 – Agency Applications/Systems and their Administration

A. Agency Applications/Systems

1. Applications are meant to support, enhance and enable business areas to accomplish their missions more efficiently and effectively. The business areas are responsible for determining their application requirements as new laws, policies and procedures are enacted or processes improved. Each Agency Head is ultimately responsible for identifying and defining the applications that are needed, how they should work and who can access them and their data. The basis of this control is the Application Administrators, who are appointed by the Agency or business heads. All applications must have an Application Administrator.

2. The Bureau of Information Technology (BIT) must provide the underlying systems and infrastructure to host these applications. This includes servers, communications, and end-user devices. BIT must also provide the physical and access security, as well as the means to recover from a system failure. To ensure continued support and security, BIT requires that applications and databases utilize standards established by BIT and Office of Administration (OA)/Office of Information Technology (OIT). Though these standards may restrict certain aspects of the look and functionality, they should not prevent an Agency from having an application that provides the necessary functionality, appearance, and control to support the Agency's business requirements.

3. The Application Administrator lists are posted on DOCNet, accessible by using the left navigation bar "Applications" link and then using the "Application Administrators" link on the Applications page. These lists inherently include all of the applications and systems that BIT supports.

4. The detailed procedures governing BIT application development and enhancement services are documented in the BIT's **Configuration Change Management Methodology Manual**, which is accessible to all BIT staff on the shared drive.

5. Requests for BIT application development and enhancement services must be evaluated and approved by the appropriate Application Administrator. The role of the Application Administrators is to act as a liaison between application users and Information Technology (IT) staff. They act as a subject matter expert for the applications they own within their area of responsibility. When needs for application changes or enhancements are identified by staff, they should be forwarded to the appropriate Application Administrator. The Administrator will determine the merit of the request based on factors such as impact on operations, productivity of staff, Agency approved initiative, mandated change, value to the business, etc. If they determine that the request is justified, they will submit the request to the BIT for further analysis to determine the estimated cost to implement the request. Once BIT returns the estimate, the Administrator will evaluate the request and either holds it for future development or request BIT to submit it on its own or in combination with other related application changes to the appropriate Agency's IT Governance Committee for project prioritization.

6. A **BIT Service Request Form** and workflow have been developed for submitting requests for BIT application development and enhancement services. The form should be completed by the person making the request and is posted, long with procedures for form completion, on DOCNet under the "Help Desk" & "Computer Forms" links. That individual will become the focal point for questions concerning the request and the definition of the detailed user requirements. The form should be completed in its entirety. Detailed information should be included so that BIT can provide an accurate estimate of the effort required to satisfy the request. If assistance is required to complete any portion of the form, the requestor may seek assistance from the Application Administrator of the system or application, the BIT Project Manager Supervisor, or the BIT Application Development Administrator. The Requestor shall email the form to the Application Administrator. If the Administrator approves the request, he/she will email the form to the CR, CEN BIT APP Req Forms mailbox. All requests must come from the Application Administrator or BIT will return the request to the Requestor.

7. Questions regarding how to use an existing application or requests for access rights to use specific applications should be directed to the Application Administrator. If the Application Administrator cannot resolve the issue, the Application Administrator will contact the appropriate BIT resource for assistance.

8. If the need for a new application is identified and an appropriate Application Administrator has not been named, the requesting Bureau or Office head will become the Administrator. Until an Administrator is named, the sponsor can submit the request directly to the CR, CEN BIT App Req Forms mailbox and BIT staff will work with the sponsor to determine the merit of the request.

B. Application Administrator

1. An Application Administrator has the authority as delegated by the Agency Head to grant access rights to the computer applications/systems to which they are assigned, and within the constraints of this policy and procedures manual, may delegate this authority to others.

2. Contractors and employees from outside agencies require approval from the Executive Deputy level (or higher) to be granted access to applications/systems within their Agency, while Application Administrators shall make final decisions when granting access to Agency employees for applications and systems for which they are responsible.

3. Whenever access is granted by an Application Administrator, they shall maintain a record of the request and the access that was granted. This can be accomplished with the Security Module for DOCInfo applications by doing a search on the user's rights and printing the screen that displays what has been assigned.

4. Some applications allow for a Local Application Administrators, while others only have a centralized Application Administrator. The Local Application Administrator grants and revokes access for an application, like an Application Administrator, but only for one location. If an application does not support the use of a Local Application Administrator, the Application Administrator takes on the role of a Local Application Administrator.

5. Application Administrators shall ensure that Local Application Administrators (where applicable) are trained on how to access and use the DOCInfo Security Admin module for Department applications and shall provide criteria and guidance for Local Application Administrations to follow in determining who should, and should not, be granted access rights to the application or system for which they are responsible.

6. Application Administrators are responsible for auditing the Local Application Administrators and the assignments of access to applications and application security role assignments at least every six months.

C. User Access to DOCInfo Applications

1. All requests for Agency employee general access to the DOCInfo applications/systems must be submitted with a FEMM request in CJINFO and reviewed by the end user's supervisor.

2. All requests for contractor or other Commonwealth employee general access to the DOCInfo applications/systems must be submitted with a FEMM request in CJINFO and reviewed by the appropriate sponsor of the person – e.g. the Agency manager who the contractor will be working for. These requests require the approval of the Executive Deputy Secretary.

3. Once general DOCInfo access has been approved and granted, request for access to restricted DOCINFO applications must be submitted in an email, along with specific justification for granting access, by the end user's supervisor to the Local Application Administrator for that application/system. A list of Application Administrators is posted on DOCNet, accessible by using the left navigation bar "Applications" link and then using the "Application Administrators" link on the Applications page.

4. The Local Application Administrator shall review all requests for access to Department applications and systems for which they are responsible and grant access to the end user if they agree with the justification provided by the end user's supervisor. Any questions regarding the need for access to an application/system shall first be discussed with the end user's supervisor. All requests for restricted applications access for contractors, non-Commonwealth employees, or non-Department Commonwealth employees must be approved by the Executive Deputy Secretary.

5. Any questions regarding the need for access for an end user that cannot be resolved after discussion with the end user's supervisor shall be referred to the Application Administrator for final disposition of the request.

6. Whenever access is granted, the Local Application Administrator shall maintain a record of the request and the access that was granted. This can be accomplished with the Security Module for DOCInfo applications by doing a search on the user's rights and printing the screen that displays what has been assigned.

7. Local Application Administrators are responsible for training end users in the use of the applications and systems for which they are responsible and for answering technical questions on the use of those applications and systems.

8. Local Application Administrators shall audit their assignments of access to applications and application security role assignments at least every six months.

D. User Access to Department Mainframe Applications

1. All requests for access to the Department mainframe applications/systems must be submitted via a FEMM request on the **Request for DOC Mainframe Computer Access** form found on DOCNet and reviewed by the end user's supervisor.

2. In the case of contractors or outside agencies, the supervisor is the Agency employee who is sponsoring them and the request will require the approval of the Executive Deputy Secretary, or higher.

3. The BIT Help Desk will create the user's account on the mainframe (if necessary) and forward the request on to the proper Application Administrator(s) if access was requested beyond the defaults.

4. The Application Administrator shall review requests for access to Department mainframe applications for which they are responsible and grant access that if they agree with the justification. Any questions regarding the need for access to an application/system shall first be discussed with the end user's supervisor.

5. Whenever access is granted, the Application Administrator shall maintain a record of the request and the access that was granted.

6. Application Administrators are responsible for training end users in the use of the applications and systems for which they are responsible and for answering technical questions on the use of those applications and systems.

7. Application Administrators shall audit their assignments of access to applications at least every six months.

E. User Access to the Pennsylvania Board of Probation and Parole (PBPP), the Office of the Victim Advocate (OVA), the Sexual Offenders Assessment Board (SOAB), and the Firearms Education and Training Commission (FETC) Applications

1. User access to PBPP applications/systems is role based and dependent on an individual's job functions.

2. Prior to the effective date of a user's appointment, PBPP Human Resources verifies and notifies Bureau of Information Technology (BIT) of that user's hire date, and provides the details necessary to explain their job functions.

3. On the effective date of a user's appointment BIT Help Desk assigns access rights to applications/systems based on that user's role and according to a pre-approved list of role-based access rights that may be granted to applications/systems.

4. The Application Administrators that are assigned by PBPP Central Office are responsible for reviewing and approving the role-based access rights that may be granted to the applications and systems for which they are responsible.

5. Application Administrators of PBPP, OVA, SOAB, and FETC applications/systems shall maintain a list of roles that have been approved for access to the applications/systems for which they are responsible and shall notify the Chief Information Security Officer (CISO) whenever changes are made to this list.

6. Any exceptions to the role-based access rights granted to PBPP, OVA, SOAB, and FETC applications/systems to any user must be reviewed and recommended by that user's supervisor, and approved by an Application Administrator, before those access rights may be assigned by BIT.

F. Chief Information Security Officer (CISO)

The BIT CISO's responsibilities include, but are not limited to:

1. question the need for access rights of an end user to any application or system;

2. review all requests for access rights for contractors and outside agencies and refer these to the Executive Deputy level (or higher) for approval/disapproval;

3. maintain a list of applications and systems, and the Application Administrators assigned to them, and ensure that these are posted on the DOCNet website;

4. maintain a list of role-based access rights to applications/systems for PBPP, OVA, SOAB, and FETC applications on the DOCNet website;

5. review and update the list of assigned Application Administrators at least every six months;

6. audit the Application Administrators, and the assignment of application security role assignments, and assignment of Local Application Administrators at least once every six moths;

7. train assigned Department Application Administrators in access to and use of the DOCInfo Security Admin module for Department applications, and shall train PBPP, OVA, SOAB, and FETC Application Administrators in their responsibilities in the process of granting role-based access rights to PBPP end users; and

8. maintain a list of applications and systems, and the Applications Administrators assigned to them, and ensure that these are posted on the DOCNet website.

Section 9 – Offender Use of Computers

A. Institutions

1. Responsibilities

   a. The Bureau of Information Technology (BIT) and Facility IT Staff (FITS) shall ensure that these procedures are adhered to and ***shall*** assist ***staff with*** determining if equipment or information has been misused or damaged by offenders.

   b. Staff are responsible for controlling, supervising, and monitoring offender computer access/***usage*** to ensure that:

      (1) offenders are only accessing ***computers and peripheral devices*** designated and marked as Offender-Use Computers;

      (2) offenders are using computers and peripheral ***devices*** for approved purposes only;

      (3) offenders are prevented from communicating with other computer systems, except ***those*** approved ***for use in education labs, library, or Correctional Industries (CI) work***; and

      (4) Department policy is adhered to with regard to offender access and use of information technology (IT) equipment, software, and systems.

2. Access

   a. Offender access to IT equipment and software is a privilege that may be rescinded at any time with or without cause and without notice. An offender shall be denied access when equipment/software misuse has occurred or is suspected.

   b. An offender may be permitted access to ***approved*** IT equipment ***and software designated/marked*** "For Offender-Use." ***A list of approved IT equipment and software will be maintained by Desktop Services***.

   c. ***An offender will be permitted internet access in the Transitional Housing Unit (THU), Reentry Services Office (RSO), and Veterans Service Unit (VSU). However, his or her internet use shall be supervised by THU/RSO/VSU staff in accordance with Section 12 of this procedures manual.***

   d. An offender ***may be*** permitted to perform work on the installation of new network cables under the direct supervision of Department staff. Offender involvement in the installation of new network cables ***shall*** be restricted to conduit installation and cable pulling tasks.

Issued: 11/3/2015
Effective: 11/10/2015

e. An offender ***shall not be*** permitted to access IT equipment, except as listed in **Subsection A.2.b.** above, and an offender ***shall not be*** permitted to access IT equipment that:

(1) contains a modem or is connected to a telephone line or a staff network. Offender access to this equipment is ***strictly*** prohibited regardless of whether or not the modem, telephone line, or network connection is active at the time the offender is accessing the equipment;

(2) is connected to a network, except for computers designated and marked "For Offender-Use" that are approved for connection to an offender network, such as in education, library, or CI. ***In all other instances***, offender access to IT network connected equipment is ***strictly*** prohibited regardless of whether or not the network connection is active at the time the offender is accessing the equipment;

(3) transfers offender generated information to other IT equipment, except for: educational purposes in classrooms, in library and laboratory settings; for educational testing as approved by the Secretary/designee, and for work purposes within CI;

(4) provides access to ***non-approved software***;

(5) controls or interacts with security systems, including but not limited to, systems that regulate door access, fire alarms, perimeter detection, counts, or other security related systems; and/or

(6) is located in an unsupervised office.

f. An offender is not permitted to:

(1) develop ***customized*** computer programs and/or applications for production use;

(2) perform information or computer program back-up routines on IT equipment, except in conjunction with coursework ***assigned*** in approved education and vocational programs (Specifically, an offender may not perform back-up routines in other places or for other work areas, ***for example***: chaplain's clerks, offender organizations, etc.);

(3) physically access communication network components including LAN hubs, routers, switches, cable patch racks, and intranet or internet cabling components that are connected to a functional cabling system;

(4) enter or maintain data that could compromise facility operations or security including, but not limited to, offender call-outs, appointments, work schedules, custody level tracking, digitized/electronic photos, photo-IDs, biometrics, offender grades, diplomas, or course completion certificates, offender payroll, offender property records, and tool inventories;

(5) physically handle, possess, or transport computer storage devices or portable storage media, except ***in conjunction with approved educational, vocational programs, THU/RSO/VSU programs***, and work in CI;

(6) make changes to or receive instruction in the configuration of operating systems or networks that are of the same type or similar to those used on production machines in the Department's facilities or operational networks;

(7) use Department provided ***IT equipment*** for personal use, except as required as part of an approved educational/vocational program to create resumes with approved software in offender libraries ***or THU/RSO/VSU***;

(8) install software on Department provided ***IT equipment except in conjunction with assigned coursework in*** an approved educational/vocational program;

(9) use software that requires Administrative or Power User rights;

(10) possess or use privately owned IT equipment, software, or portable storage media within a Department facility; ***except Department approved IT equipment (tablets) for personal*** use; and/or

(11) make repairs to Department provided IT equipment, except in conjunction with ***assigned*** coursework in an approved educational/vocational program.

3. Portable Storage Media

a. A formal system of accountability ***shall*** be established for all portable storage media used by an offender in any area ***of a Department facility***. ***All such*** media ***shall*** remain within the physical confines of the ***applicable*** area and the media ***shall*** be marked to identify the ***authorized*** area of use and that it is for offender use. All other portable storage media ***shall*** be stored away from the computers ***accessible by offenders***.

b. Media used by an offender shall be used only with ***designated*** offender-use computers. An offender shall return all portable storage media after each use to the appropriate staff ***member***. Any missing media ***shall*** be reported to ***FITS or BIT*** immediately. Master copies of computer programs shall be maintained and inventoried by FITS or BIT staff in a secured area and will not be issued to an offender. However, working copies of educational programs (software) may be used by an offender in an educational setting under the direct supervision of the teacher.

c. ***All USBs issued to offenders upon their release will be red in color. Blank USBs will be stored in the IT area and only issued to designated authorized personnel.***

d. ***The only USB permitted inside a facility shall be the facility's "DEMO" USB, which shall be marked as such, and it shall only be brought inside the THU/RSO/VSU to familiarize offenders with USBs and to train them in the proper usage of a USB. Once such offender training is complete, the DEMO USB will be returned to the facility's IT department for storage.***

e. ***Offenders shall be encouraged to submit a request for a USB drive to their THU/RSO/VSU Reentry Specialist/Reentry Parole Agent approximately two weeks prior to their scheduled release dates. An offender shall include with his or her request any diplomas, program certificates, resume(s), letters of recommendation, work reports, references, applications, and any other reentry-related documentation that he or she would like to be loaded on the requested USB drive and/or the offender shall indicate that such documentation is stored on his or her THU/RSO/VSU DVD portable storage media. The THU/RSO/VSU staff shall review the request and any documentation submitted and shall have the offender sign his or her request.***

f. ***THU/RSO/VSU staff shall designate an area specifically for scanning documents and uploading reentry USBs. Documents submitted by an offender, information stored on the offender's THU/RSO/VSU DVD portable storage media, the Reentry Resource Guide for the county of planned reentry, Reentry Resource Link information, and any other beneficial information will be uploaded onto the USB drive. Additional items to be uploaded may include Medical Records (if requested and approved per established procedures and when available electronically).***

g. ***The USB will not include personal photos, videos, or non-reentry related materials.***

h. ***The uploaded USB drive shall be etched with the offender's facility number, the three letter abbreviation for the institution that is issuing the USB drive, and the sequence number of the USB drive issued (i.e., CAM-1, CAM-2, etc.).***

i. ***After the USB is etched with the offender's information, THU/RSO/VSU staff will again access the information on the USB and verify that the information contained on the USB is that of the applicable offender.***

j. ***The etched and uploaded USB and the applicable request for the USB drive will be forwarded to the Institution's Business Office where it will be stored with the offender's personal identification documents (i.e., Driver's License/Photo ID, Social Security Card, Birth Certificate) and issued to the offender upon his or her release. Following the issuance of the USB drive to the offender, the signed request for the USB drive will be returned to the THU/RSO/VSU and it will be forwarded by THU/RSO/VSU staff to the Records Department to be included in the offender's DC-15 file.***

4. Use of Passwords

   An offender is prohibited from initiating or using passwords on computer systems and/or files, except as a non-confidential identifier needed to use an approved education computer lab. Use of a non-confidential identifier must be known to and approved by the course instructor and is not to be considered a "password" for other purposes within this policy.

5. Violation of Policy

   An offender who violates the provisions of this policy shall be subject to a misconduct in accordance with Department policy **DC-ADM 801, "Inmate Discipline."**

B. Community Corrections Centers (CCCs) *and Community Contract Facilities (CCFs)*

Any IT equipment installed at CCCs and CCFs and purchased for use by offenders using inmate general welfare funds (IGWF) or CCF funds is exempt from Section 9 of this procedures manual. The policies and procedures regarding the use of such IT equipment by offenders in CCCs and CCFs are defined in Department policy 8.3.1, "Community Corrections Security," Section 28 and in BCC-ADM 006, "Residential Services," Section 1.

Issued: 11/3/2015
Effective: 11/10/2015

Section 10 – Remote Access

A. General

1. As it relates to this section, remote access is the requirement to obtain electronic access to any secure Commonwealth, Department, Pennsylvania Board of Probation and Parole (PBPP), Office of the Victim Advocate (OVA), Sexual Offender Assessment Board (SOAB), or the Firearms Education and Training Commission (FETC) computer-based systems from outside the Commonwealth Network. This includes, but is not limited to, access via the following types of connections: broadband, WiFi, wireless, and dial-up. Remote access is provided via a Virtual Private Network (VPN) connection for approved Remote Access connections to the Commonwealth Network.

2. If remote access to any system or application (E-mail, etc.) is required, the user must submit a FEMM request through CJINFO, including detailed justification, and required information.

3. Requests for remote access must be approved by the appropriate Agency Head, Deputy Agency Head or designee, per the FEMM procedures.

4. Remote Access via VPN must be in accordance with **Information Technology Bulletin (ITB-SEC010 – Virtual Private Network Policy**.

5. All computers connecting through a VPN session to the Commonwealth internal network must be configured in compliance with all related Commonwealth and Department policies and standards using current versions of software, such as operating systems and anti-virus software, with the latest patches and upgrades. Validation and auditing processes may be used to ensure compliance with configuration standards for the Enterprise VPN Service.

B. Remote Access for Employees

1. Remote access for Department employees or contractors from a wireless or WiFi network is not authorized unless approved, in writing, by the Bureau of Information Technology (BIT) Chief Information Security Officer (CISO), and the Department's Executive Deputy Secretary.

2. Remote access for PBPP, OVA, SOAB, or FETC employees, from a wireless or WiFi network is not authorized unless approved, in writing, by the BIT CISO, the Department Executive Deputy Secretary and the appropriate PBPP, OVA, SOAB, or FETC Agency Head. Executive Deputy Secretary approval is required for PBPP, OVA, SOAB, or FETC employees, since the PBPP, OVA, SOAB, or FETC employees would be traversing the Department managed network.

Section 11 – Web Content Standards

A. General

To ensure continuity and consistency with the posting of items to the Department's external and internal web sites, the procedures outlined below have been established to comply with the requirements of the Governor's Office of Administration (OA)/Office of Information Technology (OIT) web site standards.

B. Responsibilities

1. Press Office

   The Press Office shall:

   a. develop and monitor the Department's web content standards program to ensure quality control;

   b. own the web sites' content and "look and feel;"

   c. maintain security of user permissions and access rights granted to community managers for updating all copies posted to the web sites;[1]

   d. own the information architecture or taxonomy of the web sites to ensure content is structured appropriately; and

   e. serve as administrator as the single point of control with full access rights to the web sites.

2. Bureau of Information Technology (BIT)

   The BIT will be responsible for the overall security and maintenance of the technology that supports the Department's web sites.

3. Community Managers

   a. Community Managers and back ups will be responsible to maintain local compliance with these procedures.

   b. Corrections Superintendent Assistants (CSAs) and Facility Information technology Staff (FITS) will be designated as the Community Manager and back up respectively for each facility.

   c. Community Managers and back ups for each Central Office Bureau/Office will be designated by the appropriate bureau/office director.

[1] 4-4101, 2-CO-1F-06, 2-CI-2C-2

4. Content Editors

   Individuals designated by facility Community Managers and/or Central Office Bureau/Office Director with permission to only update content on existing portlets. They cannot create or delete pages or sub-communities.

C. Web Content Management

1. The Press Secretary/designee shall:

   a. work directly with the Secretary and the Governor's Communications Office/Press Office regarding look and content;

   b. serve as webmaster of the web sites;

   c. provide training to Community Managers and back-ups;

   d. act as the primary business owner with exclusive rights to post to the public site;

   e. review and approve all content for the public site;

   f. review private site information to ensure it is posted in accordance with this procedures manual and the Governor's Style Guide;

   g. create, edit, delete communities, sub-communities, pages and portlets as needed;

   h. maintain records of all sub-communities, pages and portlets created by using the appropriate taxonomy chart;

   i. ensure posted information remains up-to-date;

   j. monitor on a regular basis public and private communities, sub-communities, pages and portlets in order to delete old items or those that are no longer necessary;

   k. ensure that public information to be posted is in line with **DC-ADM 003, "Release of Information."**

   l. work with BIT to maintain security for all communities, sub-communities, pages and portlets; and

   m. review and approve facility/bureau/office content prior to posting to the internal site.

2. Community Managers shall:

   a. create sub-communities within their respective facility or bureau/office communities. This includes creating pages and portlets and content on the portlets;

b. seek review and approval from the Portal Manager and the Press Office for any information to be posted to the public site;

c. ensure the formatting as designated in **Subsection C.1. above** is followed;

d. keep records of all sub-communities, pages and portlets created by using the appropriate taxonomy chart;

e. ensure their posted information remains up-to-date;

f. monitor on a regular basis their public and private communities, sub-communities, pages and portlets in order to delete old items or others that are no longer necessary; and

g. ensure that public information to be posted is in line with Department policy **DC-ADM 003**.

D. Web Content Format Standards

1. Text

a. ALL CAPS only shall be used to highlight headers and/or key words within a document or as an acronym.

b. At no time shall all content on a page be in all caps.

(1) permissible: DOC, DCC, SNU, RHU;

(2) permissible: After the assault the inmate was placed in the RHU. Staff is conducting an investigation. Questions should be directed to the Security Office; and

(3) NOT permissible: AFTER THE ASSAULT THE INMATE WAS PLACED IN THE RHU. STAFF IS CONDUCTING AN INVESTIGATION. QUESTIONS SHOULD BE DIRECTED TO THE SECURITY OFFICE.

c. Titles shall be in upper and lower case (as shown above). At no time shall a title be in all caps.

(1) permissible: Facility News; and

(2) NOT permissible: FACILITY NEWS.

d. Font: Veranda.

e. Font Size

(1) title: 5 (shall be bolded and centered);

(2) subtitle, if necessary: 4; and

(3) text: 3.

f. Font color: Black.

g. There shall be no deviation from the font or font sizes and there shall be no flashing or scrolling test.

2. Photos/Graphics

a. Photos within documents that will be uploaded/posted (such as those in Word or PDF documents) are permitted.

b. Photos and/or graphics that will be posted in portlets should be used sparingly. If photos and/or graphics are used, ensure that their proportion is not skewed or stretched when resizing them.

c. At no time shall a photo or graphic ever be larger than 4”x6”.

d. No animated graphics or graphics deemed inappropriate will be permitted.

e. To view photos taken at an event, it is encouraged that the photos be inserted into a Word document and that the document is then converted to PDF for posting. In a Word or PDF document, the size of photos will not be limited.

f. The goal is to conserve server space and to ensure consistency throughout the web site. The uploading and posting of photos/graphics to actual portlets takes up space, thus inserting photos into Word or a PDF document helps with this.

Section 12 – Institution Offender Internet Access Procedures

A. Application Specific Internet Access

The applications on some offender devices require access to a limited number of internet sites to function properly. These applications will be classified by the functional purpose of the application (e.g. Academic Labs, GED labs, etc.). The Bureau of Information Technology (BIT) will identify these applications and the internet sites accessible from the devices associated with these applications. This information will be maintained by BIT and will be posted on DOCNet. The devices associated with these applications are not considered part of the Transitional Housing Unit (THU), Reentry Services Office (RSO), and Veterans Service Unit (VSU) computer labs and are not subject to the policy and procedures in **Section 12** of this procedures manual.

B. THU/RSO/VSU Computer Labs

1. Computer labs will be established at Department of Corrections (DOC) institutions for use by offenders in their THU/RSO/VSUs.

2. THU/RSO/VSU computer labs will be granted access to the internet as defined in **Section 3** of this procedures manual.

C. THU/RSO/VSU Lab Security Requirements

1. The space allocated for each reentry computer lab must facilitate the ability for a single staff member to physically observe all computers and printers in that lab simultaneously.

2. The computers must be powered off and secured when there is no direct physical staff oversight. The preferred approach is to dedicate a lockable room for the computers. In cases where there are insufficient resources to designate a lockable room, it is acceptable to render the computers unusable by removing and securing all keyboards and mice when staff are not providing direct physical oversight.

3. Offenders must be directly supervised by designated staff while utilizing these computers and staff must physically monitor offenders' computer use while the offenders are using computers and printers.

4. End user IDs and passwords will be assigned to each offender computer. End user IDs will be established in accordance with the computer configuration procedures for the THU/RSO/VSU labs. The Unit Manager/designee will assign a single staff member to be responsible for password administration on all computers in a specific lab. The Unit Manager may approve the use of a single password for all offender internet computers within a specific lab at his or her discretion. End user password administration must adhere to the requirements listed below.

Issued: 11/3/2015
Effective: 11/10/2015

a. Passwords must be changed at least every 60 calendar days.

b. Passwords may be stored in an electronic file maintained by the THU/RSO/VSU staff (e.g. Excel Spreadsheet, Word Document, etc.). Electronic files containing password information shall be password-protected and stored on staff server-based file storage resources. Passwords may not be recorded on any other media, physical or electronic.

c. Passwords shall be at least eight characters in length and shall include at least one each of the following: numbers, lower-case letters, upper-case letters, and non-numeric/non-alphabetic characters.

d. Passwords shall not be entered into any device in the presence of offenders.

D. Offender Eligibility and Lab Scheduling

1. Eligible offenders must submit a **DC-135A, Inmate Request to Staff Member** to the designated staff to request internet lab.

2. Designated staff must confirm that a signed copy of **Internet Acknowledgement – Offender (Attachment 12-A)** is on file before scheduling an offender for computer lab time.

3. Designated staff shall finalize the schedule for offender internet computer lab time using **Offender Internet Lab Scheduling Sheet (Attachment 12-B)** and inform the requesting offender of his or her approved time slot.

4. Lab time will be scheduled on a "first-come, first-serve" basis with those offenders with upcoming release dates receiving priority.

5. Individual offender sessions shall be made available in one-hour increments based on staff availability to supervise.

E. Offender Internet/Email End User Agreement Procedures

1. Unit Managers shall maintain a copy of all Offender Internet/Email End User Agreements on the unit. The storage location must be securable and accessible to designated staff assigned responsibility for reviewing these agreements.

2. Prior to using the lab for the first time, designated staff shall review the Offender Internet/Email End User Agreement with the offender. The offender and staff member shall both sign the agreement at the conclusion of this review.

3. The designated staff shall provide a copy of the signed agreement to the offender, file another copy of the signed agreement in the offender's file, and file the original signed agreement in the central repository in offender number sequence.

F. Offender Internet Computer Lab Daily Usage Procedures

Designated staff shall complete the following tasks on a daily basis:

1. Open the lab in accordance with the schedule.

2. Login to the computer(s) using the user name and password designated for each computer.

3. Create a new log entry in the **Offender Internet Lab Log Sheet (Attachment 12-C)** that includes the following:

   a. starting staff initials;

   b. start time;

   c. computer number;

   d. offender number;

   e. offender name; and

   f. the first entry for a given day must include the facility, date, and day fields at the top of the log sheet.

4. Maintain direct observation of all computers that have been powered-on and logged into.

5. Logoff any computer that is no longer in use and update the corresponding log entry by completing the fields listed below:

   a. end time; and

   b. ending staff initials.

6. At the conclusion of the last lab session, secure the computers in accordance with the lab security requirements of this policy and provide the original **Offender Internet Lab Log Sheet** to the Unit Manager.

7. Store the **Offender Internet Lab Log Sheets** in a secure location keeping all logs in chronological sequence. **Offender Internet Lab Log Sheets** shall be maintained on file for at least 90 days. Logs exceeding that retention period shall be disposed of using standard records retention/disposal procedures.

G. Offender Data Storage Requirements

Offenders will have the need to store information associated with their internet access (e.g. resumes, certifications, employment documentation, etc.). Digital versatile discs (DVD's) will be used to accommodate this need. The policy and procedures regarding offender use of portable storage media are defined in **Section 9** of this procedures manual.

H. Responsibilities

1. Facility Manager shall:

    a. designate staff responsible for Offender Internet Computer Lab Daily Usage Procedures. These staff may include Unit Managers, counselors, treatment specialists, social workers, or other program staff;

    b. allocate space for computers and printers to establish THU/RSO/VSU lab(s) in accordance with the THU/RSO/VSU Lab Security Requirements;

    c. provide electric power, data cabling, and furniture for the computers and printers in the THU/RSO/VSU lab(s); and

    d. allocate funding for ongoing maintenance and support of THU/RSO/VSU lab equipment:

2. Facility IT Staff shall provide server-based file storage resources for the storage and retrieval of end user password information in accordance with THU/RSO/VSU Lab Security Requirements.

3. Unit Manager shall:

    a. designate facility staff responsibilities for end user password administration on all lab computers;

    b. maintain a file of **Offender Internet Lab Log Sheets,** in accordance with Offender Internet Computer Lab Daily Usage Procedures, and respond to all requests for **Offender Internet Lab Log Sheets**;

    c. establish and implement procedures in accordance with Offender Internet/Email End User Agreement Procedures; and

d. designate hours of availability for lab use with the goal of making the lab available a minimum of 15 hours per week contingent upon operational requirements of the facility.

4. Designated Facility Staff shall:

a. operate THU/RSO/VSU labs in accordance with Offender Internet Computer Lab Daily Usage Procedures;

b. administer end user passwords on THU/RSO/VSU lab computers in accordance with THU/RSO/VSU Lab Security Requirements;

c. administer the offender selection process and the lab scheduling process in accordance with Offender Eligibility and Lab Scheduling;

d. administer Offender Internet/Email End User Agreements in accordance with Offender Internet/Email End User Agreement Procedures; and

e. assist offenders with the use of THU/RSO/VSU lab equipment, internet access/navigation, and portable media data storage.

Agency/Agencies – the Department of Corrections (DOC), the Board of Probation and Parole (PBPP), the Office of the Victim Advocate (OVA), the Sexual Offender Assessment Board (SOAB), and the Firearms Education and Training Commission (FETC).

Agency Head – the Secretary of Corrections (DOC), the Chairman of the Board of Probation and Parole (PBPP), the Office of the Victim Advocate (OVA), the Executive Director of the Sexual Offender Assessment Board (SOAB), and the Executive Director of the Firearms Education and Training Commission (FETC).

Application Administrator – The individual(s) responsible for a ***particular*** business area with business functions that are supported by computer applications/systems assigned to him/her and of which he/she is considered the owners. An Application Administrator is responsible for making recommendations to agency heads for changes to Agency policies and procedures ***regarding*** the business practices in his or her areas of responsibility and for approving the development of and enhancements to applications/systems that support these business practices.

Application Administrator Password – A confidential alphanumeric code used to logon to a computer or system to perform restricted functions for specific computer applications/systems, such as assigning users, creating backup files, loading or restoring data from CD-ROMs or other media.

Application and Application System – An application is a computer program or programs that supports a specific business function. A simple business process, such as Call Outs, has one function and is supported by one application. A more complex business process, such as Parole Supervision, combines multiple business functions, requires a system of applications to support it, and may be referred to as a system or an application system.

Basic Input Output System (BIOS) – Initial instruction set used during the startup of a computer system.

BIT – Bureau of Information Technology

BIT Field Services Section – A section of BIT that oversees the operation of the centralized Help Desk and provides direction to the Business Managers and FITS related to IT support.

Business Manager – The manager located at a Department facility, who has overall responsibility for running the business office for that facility, to include supervising the FITS. He or she works with the Facility Manager(s) at the supported facilities, FITS and BIT to ensure that IT is used effectively and in accordance with Commonwealth and the Agencies' policies.

Central Office – The Agency offices that house the centralized functions of the Agencies.

Central Office Managers – Central Office bureau and office directors and division chiefs.

Chief Information Security Officer (CISO) – The individual responsible for strategic planning, policy formulation, implementation, and ongoing security of all information systems and data communications programs supported by the Bureau of Information Technology (BIT).

CIO – Chief Information Officer

Complementary Metal Oxide Semiconductor (CMOS) – Storage area for the initial instruction set used during the startup of a computer system.

Computer Inventory – The Department's official central inventory of Information Technology Equipment and Software as maintained by the BIT.

Confidential Information – Information that is protected from disclosure by law, is treated or designated by law as confidential, specifically has been designated as confidential by the Department or another agency of the Commonwealth, as well as information the disclosure of which could threaten the security of the Department or any Departmental facility, facilitate an escape or create a danger to a member of the staff, a contractor, the public, or inmates.

Copyright – Legally enforceable ownership rights in published intellectual property, such as software. The copyright-holder for a piece of intellectual property possesses the exclusive rights to reproduce and distribute the intellectual property and power to grant the rights of reproduction and distribution to others.

CWOPA – Commonwealth of Pennsylvania

Data Communications Network – A telecommunications medium and associated components responsible for the transportation of computer information from one location to another.

Desktop Computer – Desktop or tower configuration microcomputers used by employees, inmates, contractors, and individuals within the Department.

DOCInfo – The Department's official intranet (internal) application web site – i.e., it consists of application systems.

DOCNet – The Department of Corrections' official intranet web site.

Document Password – A password used to restrict access to a single document.

E-mail – Electronic mail.

Employee – Full-time, part-time, limited term wage, intern, or contracted staff employed by the Department.

Facility – A physical location encompassing one or more offices and buildings. Examples are Central Office, State Correctional Institutions, Parole Field Offices, and Community Corrections Centers.

Facility Application Administrators – See Local Application Administrators.

Facility Information Technology Staff (FITS) – Persons in an Information Technology classification assigned to work in facilities or a particular Bureau/Office that have been approved/trained by the BIT to perform tasks outlined in this policy.

Facility Manager – The person who has overall responsibility for a particular facility (State Correctional Institution, Parole Field Office, Community Corrections Center, etc.).

Head of the Appropriate Agency (HoAA) – the Secretary of Corrections (DOC), the Chairman of the Board of Probation and Parole (PBPP), the Victim Advocate (OVA), the Executive Director of the Sexual Offenders Assessment Board (SOAB), and the Executive Director of the Firearm, Education, and Training Commission (FETC).

Information Security Administrator (ISA) – The individual who assists the CISO in planning, designing, implementing, and maintaining system security standards, policies, procedures and access to agency systems.

Information Security Officer/Administrator (ISO/ISA) – The individual responsible for the security of both Department's and PBPP's electronically stored information.

Instant Messaging – Synchronous or real time exchange of text messages, files, photos, and other data over the internet.

ITGC – the Information Technology Governance Committee.

Local Application Administrator – An individual assigned to perform restricted functions for specific computer applications/systems, such as assigning users certain levels of functionality or access rights at a specific field site, office, or facility outside of Central Office. These individuals understand the business functions and processes that these applications/systems support, as well as the use of the applications/systems themselves. (The Security Admin module in DOC Info refers to Local Application Administrators as Facility Application Administrators.)

Local IT Staff – The IT staff responsible for the direct support of the end-user IT assets. At the Department and PBPP Central Offices, this is the BIT Help Desk. At the Facilities (Department and PBPP offices), this is the assigned FITS. At the Community Corrections and Parole field offices, this is the nearest facility FITS.

Microcomputer – Programmable desktop or portable (handheld, laptop, palmtop, etc.) computers each of which may have its own microprocessor, operating system and application software. These units can function in a standalone mode, as part of a Local Area Network (LAN), and/or as a terminal emulation device connected to a mainframe computer.

Office of Administration (OA) – An office under the Governor's jurisdiction that, among other things, directs the Commonwealth's deployment of technology.

OA/OIT – OA via its Office for Information Technology.

Operating Systems – Computer programs that run other computer programs. They perform basic tasks, such as responding to input, displaying output, organizing files and directories.

They also work devices such as disk drives and printers. (Windows 2000 and Windows XP are examples of operating systems.)

OVA – the Office of the Victim Advocate.

Password – An alphanumeric code used to log onto a computer or system to access its services, files, and computer programs. Use of a password is intended to limit the persons who can access certain functions or information.

Personal Computer – See definition of a microcomputer.

Peripherals – A general term of any of the external devices (mouse, keyboard, CD/DVD reader/writer, printer, scanner, etc.) attached to Information Technology Equipment.

Personal Password – A password used in conjunction with a person's own User-ID to provide access to computer systems.

Portable Computing Devices – Any computer small enough to carry. They include, but are not limited to, Portable Digital Assistants (PDAs), notebook computers, pen tablet PCs, Palm Pilots, laptop computers, Microsoft Pocket PCs, RIM Blackberries, MP3 players, text pagers, smart phones, and other similar devices. Within this document, notebooks and pen tablet PCs will all be referred to as laptop computers or laptops.

Portable Media Storage Devices – Any type of transportable media that can be used to move images, information, photos, software, or video to or from IT equipment or networks. Examples include CDs, DVDs, external hard drives, flash drives, flash keys, flash media cards/drives, flash memory cards, floppy disks, jump drives, magnetic tapes, memory cards, memory keys, memory drives, memory sticks, pen drives, removable hard drives, thumb drives, USB connectable storage devices, and FireWire connectable storage devices, etc. This includes USB pocket music players and similar computer connectable devices even if not intended for that use.

Restricted Email – Email that enables an employee to send and receive written messages and attachments to only those users in CWOPA Global Address List. This is the default for all DOC CWOPA accounts.

Screensavers – Computer programs designed to automatically place graphics, pictures, etc on a computer monitor in place of applications or data when it detects that a computer has not actively been used for a certain period of time. Also included are computer programs designed, for amusement purposes, to place images or animated characters on a screen either in place of or along with applications or data.

Secure Area – An area in which inmates are not assigned to work and which is always locked when staff are absent.

Secure Perimeter – Barrier that defines the inner-compound of a correctional facility.

Secure Storage – A locking desk, file cabinet or similar non-portable storage.

SOAB – the Sexual Offender Assessment Board.

Staff – Any employee of the Commonwealth of Pennsylvania or any person working under contract with the Commonwealth or other person to whom this policy applies, except inmates.

Strong Password – A Password that:

- must be a minimum of seven characters:
- must be composed of at least three of the following types of characters,
  - Uppercase letters (A, B, C, ….)
  - Lowercase letters (a, b, c, ….)
  - Numbers (1, 1, 2, 3, ….9)
  - Special characters (#, other punctuation marks); and
- may never contain the user ID, nor any part of the user's full name.

System Administrator Password – A confidential alphanumeric code used to logon to a computer or system to access restricted functions such as operating systems and network configuration settings.

TID – the Technical Infrastructure Division, which is a division of DOC BIT.

TRC – the Technical Review Committee.

Unrestricted E-mail – E-mail that may be sent to or received from anywhere (E-mail not limited to just addresses within the Commonwealth of PA's E-mail system).

User-ID – A unique identifier (user name) used to identify a person who logs onto a computer. Generally, User-IDs are not confidential.

Virtual Private Network (VPN) – A computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the internet) instead of by physical wires.

Virus – A computer program that is designed to copy itself, attach itself to other computer programs, and spread onto other computers and then to perform functions which annoy the user, interrupt normal computer operations, destroy files or access/copy information without authorization. Viruses are often unintentionally downloaded from web sites or passed via portable storage media or through attachments to E-mail.

Wireless Communication Device – A device that transmits and receives data, text, and/or voice without being physically connected to a network. This definition includes, but is not limited to, such devices as cellular telephones, pagers, wireless internet services, wireless data devices (e.g., Blackberry devices), and cellular telephone/two-way radio combination devices. This

definition does not include the radio devices that interface with the 800 MHz Statewide Radio System.

Workstation – A microcomputer connected to a network for the purpose of utilizing network resources.